z/OS Communications Server
2.5

IP and SNA Codes

SC27-3648-40

Note:

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 833.

Last updated: 2021-09-11

© Copyright International Business Machines Corporation 2000, 2021.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures ..... **xxxi**

Tables ..... **xxxiii**

About this document ..... **xxxv**
Who should read this document xxxv
How this document is organized xxxv
How to use this document xxxvi
How to contact IBM service xxxvi
Conventions and terminology that are used in this information xxxvi
Prerequisite and related information xxxvii

Summary of changes for IP and SNA Codes ..... **xliii**
Changes made in z/OS Communications Server Version 2 Release 5 xliii
Changes made in z/OS Communications Server Version 2 Release 4 xliii
Changes made in z/OS Communications Server Version 2 Release 3 xliii

Chapter 1. SNA sense codes **1**
Sense codes 1
08XX (request reject) 2
10XX (request error) 98
20XX (state error) 120
40XX (RH usage error) 123
80XX (path error) 124
A0XX (RTP sense data) 135
FFXX (HPR sense data) 141
SNA sense field values for RPL-based macroinstructions 143
3270 SNA and non-SNA device sense fields 144

Chapter 2. Return codes for VTAM macroinstructions **147**
ACB OPEN and CLOSE macroinstruction error fields 147
OPEN macroinstruction error fields 147
CLOSE macroinstruction error fields 150
RPL RTNCD and FDB2 return code combinations 151
RTNCD and FDB2 information for LU 6.2 170
RCPRI and RCSEC return codes for LU 6.2 172
LAN channel station error return codes 206
Byte 0—LAN general classifications 206

Chapter 3. Data link control (DLC) status codes **223**

Chapter 4. CSM monitor IDs **261**

Chapter 5. VTAM status codes **265**
Resource status codes and modifiers 265
Resource state code categories 265
Resource state code values 266
Resource status modifiers (positions 4 and 5) 282

Resource status field information (positions 6–10)....283
Session states and modifiers....284
Session state modifiers and suffixes....284
Session initiation states....284
Session termination states....290
Session status modifiers (positions 6–8)....291

Chapter 6. VTAM wait state event codes and IDs....293
Codes 0102–010C (configuration services LQAB group)....293
Event Code 0102....293
Event Code 0103....293
Event Code 0104....293
Event Code 0105....294
Event Code 0106....294
Event Code 0107....294
Event Code 0108....294
Event Code 010A....295
Event Code 010B....295
Event Code 010C....295
Codes 0201–020D (I/O LQAB group)....295
Event Code 0201....295
Event Code 0202....296
Event Code 0203....296
Event Code 0204....296
Event Code 0206....296
Event Code 0208....297
Event Code 0209....297
Event Code 020B....297
Event Code 020C....297
Event Code 020D....298
Codes 0301–0306 (logical unit services LQAB group)....298
Event Code 0301....298
Event Code 0302....298
Event Code 0304....298
Event Code 0305....299
Event Code 0306....299
Codes 0401–0409 (physical unit services LQAB group)....299
Event Code 0401....299
Event Code 0402....299
Event Code 0403....300
Event Code 0404....300
Event Code 0405....300
Event Code 0406....300
Event Code 0407....301
Event Code 0408....301
Event Code 0409....301
Codes 0501–0503 (network operator services LQAB group)....301
Event Code 0501....301
Event Code 0502....302
Event Code 0503....302
Codes 0601–0610 (session services LQAB group)....302
Event Code 0601....302
Event Code 0602....303
Event Code 0603....303
Event Code 0604....303
Event Code 0605....303
Event Code 0606....303

Event Code 0607....304
Event Code 0608....304
Event Code 0609....304
Event Code 060A....304
Event Code 060B....305
Event Code 060C....305
Event Code 060D....305
Event Code 060E....305
Event Code 060F....305
Event Code 0610....306
Code 0701 (session services LQAB 2 group)....306
Event Code 0701....306

Chapter 7. VTAM abend codes....307
Abend code 0A7....307
Abend code 0A8....307
Abend code 0A9....309
Abend code 0AA....313
Abend code 0AB....313
Abend code 0AC....314
Abend code 0AD....315

Chapter 8. ATM network-generated cause and diagnostic codes....317
ATM network-generated cause codes....317
ATM network-generated coding standard....323
ATM network-generated cause location....324
ATM network-generated diagnostic codes....324
Diagnostic code for cause codes 1, 2, and 49....324
Diagnostic code for cause code 21....325
Information element identifier....326
ATM user cell rate subfield identifier....327
Virtual path connection identifier (VPCI) and virtual channel identifier (VCI)....327
Message type....328
Timer number....330

Chapter 9. SNA coupling facility user reason codes....333
Rebuild start reason codes....333
00000108*x* storage shortage....333
00000112*x* loss of connectivity....333
00000114*x* list number expansion....333
Rebuild stop reason codes....333
00000100*x* response failure....333
00000104*x* local repopulation failure....333

Chapter 10. TCP/IP codes....335
GDDMXD/MVS abend codes....335
102....335
103....335
104....336
105....336
MVS platform (MVPMAIN) completion codes....337
1*xx*....337
200....338
316....338
516....339
600....339
7*xx*....340

8*xx* ... 340
9*xx* ... 341
MVS platform (MVPXVI) completion codes ... 341
52 ... 341
3016 ... 342
4000 ... 342
5000 ... 343
70*xx* ... 344
SNALU6.2 abend codes ... 344
1 ... 344
100 ... 344
200 ... 345
210 ... 345
220 ... 346
300 ... 346
310 ... 346
320 ... 347
331 ... 347

Chapter 11. SNMP pe_error messages ... 349
Class/ID mismatch in constructor ... 349
Not a constructor form ... 349
Not a primitive form ... 349
Out of memory ... 349
Overflow ... 350

Chapter 12. SNMP ps_error messages ... 351
End of file ... 351
End of file reading extended ID ... 351
End of file reading extended length ... 351
Indefinite length in primitive form ... 351
Length Mismatch ... 352
Out of memory ... 352
Overflow in ID ... 352
Overflow in length ... 352
XXX ... 353

Chapter 13. Sockets and sockets extended return codes (ERRNOs) ... 355
Sockets return codes (ERRNOs) ... 355
Sockets extended ERRNOs ... 366

Chapter 14. TCP/IP abend 3C5 reason codes ... 371
001: Bad Load ... 371
002: UCB DEQ Failed ... 371
003: MVPDG7C Logic error 1 ... 371
004: MVPDG7C Logic error 2 ... 371
005: MVPIOINT Circular Q ... 371
006: Operator Forced Dump ... 372
007: Get of TNF area failed ... 372
008: Zero ptr ... 372
009: Cannot locate TNF SSCT ... 372
010: Raclow allocate failed ... 372
011: Raclow free failed ... 373
012: GARB routine allocation failure ... 373
013: VTWK Free error ... 373
015: Zero token invalid bug ... 373
016: Unqueue - entry not found ... 373

017: Message complete not done here..... 374
018: Bug - wrong type to Q_IUCV_Int..... 374
019: Count going negative.....374
020: Bad interrupt type being Queued..... 374
021: Caught local lock held in xiuc..... 374
022: Logic error in DoQr MVPXIUC.....375
023: GARB routine allocation failure..... 375
024: Lock not held error..... 375
025: Count going negative.....375
026: Internal error in path counting..... 375
027: GARB routine allocation failure..... 376
028: Unqueue - entry not found.....376
031: Wrong ASCB..... 376
032: Caught Local lock held in xtnf.....376
033: Unqueue - entry not found.....376
034: Alloc user data failed..... 377
035: Alloc SRBS failed.....377
036: Freemain of SRB failed.....377
037: Getlock for 0 asid..... 377
038: Local lock not held error..... 377
039: Local lock held.....378
040: Local lock should be held.....378
041: Too many locks held.....378
042: User lock already held excl..... 378
043: Two user locks in read only.....378
044: Upgrade lock by wrong TCB.....379
045: User lock not held excl.....379
046: Already holding user lock.....379
047: User lock is not held excl..... 379
048: More than two user locks error.....379
049: holding other user lock exclusively..... 380
050: Already held the local lock.....380
051: Must hold user lock first.....380
052: Path lock already held exclusive.....380
053: Already holding path lock..... 380
054: Lock already held..... 381
055: Another subordinate lock held..... 381
056: Freelock for 0 asid.....381
057: Freeing not-held lock..... 381
058: Subordinate not free..... 381
059: Local lock was not held.....382
060: Caught local lock held in xvmc..... 382
061: GARB routine allocation failure..... 382
062: Unqueue - entry not found.....382
063: YSRB Freemain of SRB failed.....382
101: Interrupt when INT_GETN. AddUserNote rc not zero.....383
102: Interrupt when INT_PECB. Circular buffer wrapped..... 383
103: In SQLSUBx-TASK. "TODO" not FETCH a row -or- CLOSE DOWN.....383
104: In PUTVTAM. New VTAM PUT addr equals VTAM GET addr.....383
105: In IUCVRUPT. New IUCV PUT addr equals IUCV GET addr.....383
106: Usage error.....384
107: Session Type..... 384
108: Max RU size..... 384
109: Storage for path index table..... 384
110: IUTIL Init Error.....384
111: Missing CONNBLOK.....385
112: OPENACB failure..... 385
113: SETLOGON failure..... 385

502: UNITCHEC Freemain error....385
503: TAPECHEC FREEMAIN ERROR....385
504: DYNALLOC (SVC 99) failure....386
505: CCALL: Data copy allocate failure....386
506: GARB routine allocate failure....386
507: Unexpected GTTERM Return Code....386
508: Unexpected STFSMODE Return Code....386
509: Unexpected TPG Return Code....387
510: Unexpected Return Code from TGET after TPG....387
511: Invalid device for Diagnose 8C....387
512: Unexpected GTTERM Return Code in Diagnose 8....387
513: Invalid virtual device number....387
514: Unexpected Diagnose Request....388
515: Invalid WSF Data....388
516: Invalid Query Data....388
517: Unexpected STFSMODE Return Code....388
518: Bad STTMPMD Return Code....388
519: Bad STTMPMD Return Code....389
520: Unexpected TPUT Return Code....389
521: Unexpected TGET Return Code....389
522: Unexpected TGET Return Code....389
523: Unexpected TPG Return Code for read buffer....389
524: Unexpected TGET Return Code....390
525: Unexpected Diagnose 58 OpCode....390
526: Error allocating write buffer....390
527: Error allocating read buffer....390
528: Unexpected STFSMODE Return Code....390
529: Error freeing write buffer....391
530: Error freeing read buffer....391
531: Bad STTMPMD Return Code....391
532: Unexpected STFSMODE Return Code....391
533: MVSCLOSE DCB=0....391
534: MVSPOSIT zero DCBptr....392
535: BFREAD DCB=0....392
536: SLOWSFRE DCB=0....392
537: BFWRITE DCB=0....392
538: SFWRITE DCB=0....392
539: Null=2....393
540: Null=1....393
541: WRITEBLOck DCB=0....393
542: WRITEBLOck DCB=0....393
543: BLOKREAD DCB=0....393
544: BLOKWRIT DCB=0....394
545: BLOKINFO DCB=0....394
546: MVSAPPEN DCB=0....394
547: MVPCFIO (MVSMEMLI)....394
548: DSLIS Free=1....394
549: Bad Locate parms....395
550: DISLIS Free=2....395
551: Bad return code from PUTGET....395
552: Unexpected TGET Return Code....395
553: Bad RC from STIMERM SET....395
554: Bad Return Code from IKJEFTSR....396
555: Bad Return Code from IKJEFTSR....396
556: CXSEM: Data copy free failure....396
557: This return code should not occur....396
558: GETJOBID ZERO DCBPTR....396
559: Unrecognized Dsorg....397

560: Incorrect DSCB obtained ... 397
561: Obtain error ... 397

Chapter 15. TCP/IP abend 422 reason codes ... 399
04FD ... 399
04FE ... 399
04FF ... 399

Chapter 16. TCP/IP abend 4C5 reason codes ... 401
03FE: TcpTerminatedFail ... 401
03FF: TcpTerminatedNorm ... 401
0401: TcpBadEntryCode ... 401
0402: TcpUnexpectedErr ... 401
0403: TcpInBadStack ... 401
0404: TcpLostOMPROUTE ... 401
0405: TcpSysplexUnresponsive ... 402
04C1: TcpINEcode ... 402
04C2: TcpINDspservC ... 402
04C3: TcpINAleservA ... 402
04C4: TcpINAleservE ... 402
04C5: TcpINAleservD ... 402
04C6: TcpINDspservD ... 402
04C7: TcpINTcbToken ... 402
04C8: TcpINLxres ... 403
04C9: TcpINAxset ... 403
04CA: TcpINEtcre ... 403
04CB: TcpINEtcon ... 403
04CC: TcpINEstae ... 403
04CD: TcpINBadVSMLoc ... 403
04CE: TcpINBadLoad ... 403
04CF: TcpINEtdes ... 403
04D0: TcpINBadParm ... 404
04D1: TcpINCsvquery ... 404
04D2: TcpINPgser ... 404
04D3: TcpINAxres ... 404
04D4: TcpINAsext ... 404
04D5: TcpINAsxTcbToken ... 404
04D6: TcpINLxfre ... 404
04D7: TcpINAttach ... 404
04D8: TcpINBadDelete ... 405
04D9: TcpINAxext ... 405
04DA: TcpINNoTseb ... 405
04DB: TcpINBadDirectedLoad ... 405
04DC: TcpInBadEZBITCOM ... 405
05C0: TcpS2Ecode ... 405
05C1: TcpSMLatchSetExists ... 405
05C2: TcpSMLatchCreateOutOfStorage ... 405
05C3: TcpInIsglcrt ... 406
05C4: TcpInvCellStart ... 406
05C5: TcpInAleserv ... 406
05C6: TcpInvReleaseReq ... 406
05C7: TcpInCsrpbld ... 406
05C8: TcpInCsrpexp ... 406
05C9: TcpInvCellToken ... 406
05CA: TcpInvCellAddr ... 406
05CB: TcpInCsrpget ... 407
05CC: TcpInCsrpfre ... 407

05CD: TcpInCsrpqpl..... 407
05CE: TcpInCsrpcon..... 407
05CF: TcpInCsrpact..... 407
05D0: TcpCBInvalidStack..... 407
05D1: TcpCBStackOverflow..... 407
05D2: TcpOutOfMasterCells..... 407
05D3: TcpOutOfMasterCBCells..... 408
05D4: TcpOutOfStackCells..... 408
05D5: TcpInvalidCpoolId..... 408
05D7: TcpSmEstae..... 408
05D8: TcpInCsrpqex..... 408
05D9: TcpInCsrpdac..... 408
05DA: TcpInCsrpdis..... 408
05DB: TcpInLength..... 408
05DC: TcpInDataSpaceGroupID..... 409
05DD: TcpInDataSpaceAlet..... 409
05DE: TcpInDataSpaceStoken..... 409
06C1: TcpTSEstae..... 409
06C2: TcpTCMLLockHeld..... 409
07C1: TcpLAObtHier..... 409
07C3: TcpLARelHier..... 409
07C5: TcpLAObtFail..... 409
07C7: TcpLARelFail..... 410
07C9: TcpLAFreLocked..... 410
07CB: TcpLAInvTlcb..... 410
07CD: TcpLAInvLmca..... 410
07CF: TcpLAInvLmqe..... 410
07D1: TcpLAAllocLatch..... 410
07D3: TcpLAObtDelete..... 410
07D5: TcpLAInvConTok..... 410
07D7: TcpLAAllocLS..... 411
07D9: TcpLAInvTcb..... 411
08C1: TcpSMGetCell..... 411
08C3: TcpSMGetCellD..... 411
08C5: TcpSMFreeCellZero..... 411
08C7: TcpSMGetCellInUse..... 411
08C9: TcpSMFreeCellInUse..... 411
08CB: TcpLALatchSetInUse..... 411
08CD: TcpSMFreeCellCirc..... 412
08FF: TcpOPInvEye..... 412
1001: TcpSKBadVerb..... 412
1101: TcpSKMsgNotAvailable..... 412
1102: TcpSKMsgHoldFailed..... 412
1103: TcpSKMsgReleaseFailed..... 412
2000: TcpitProcStackExceeded..... 412
2001: TcpitLockObtNotInit..... 412
2002: TcpitLockObtLevelHeld..... 413
2003: TcpitLockObtStatusChange..... 413
2004: TcpitLockObtHierarchy..... 413
2101: TcpitLockRelNotInit..... 413
2102: TcpitLockRelNotHeld1..... 413
2103: TcpitLockRelLevelHeld..... 413
2104: TcpitLockRelNotHeld2..... 413
2105: TcpitLockRelNotHeld3..... 413
2201: TcpitLockTstNotInit..... 414
2301: TcpitLockRelAllAbend..... 414
2401: TcpitLockSusError1..... 414
2402: TcpitLockSusError2..... 414

2403: TcpitLockSusError3....414
2500: TcpitStorNoStorage....414
2501: TcpitStorNoCSMstorage....414
2502: TcpitStorBadHeader....414
2503: TcpitStorBadTrailer....415
2504: TcpitStorBadParm....415
2505: TcpitStorCSMtooLarge....415
2506: TcpitStorNotAllocated....415
2507: TcpitStorNoPrivStorage....415
2508: TcpitStorECSALimit....415
2509: TcpitStorPoolLimit....415
2600: TcpitDUbadParm....415
2601: TcpitDUSusError1....416
2701: TcpitTimerBadTQE1....416
2702: TcpitTimerCanError1....416
2703: TcpitTimerCanError2....416
2704: TcpitTimerBadTID1....416
2705: TcpitTimerBadTQE2....416
2706: TcpitTimerSetFailed....416
2707: TcpitTimerBadState1....416
2708: TcpitTimerBadTID2....417
2709: TcpitTimerBadTQE3....417
270A: TcpitTimerBadState2....417
2801: TcpitTrrStackFull....417
2900: TcpPatTreeCorrupted....417
2901: TcpPatTreeKeyTooLarge....417
2902: TcpPatTreeBadParm....417
2A00: TcpHashTabUnbalanced....417
3001: TcpSTKattLoop....418
3002: TcpSTKblkngArrInvalid....418
3003: TcpSTKPtreeRecovery....418
3004: TcpSTKLoopIutlChain....418
3005: TcpSTKMProtoInvalid....418
3006: TcpSTKLoopIutlDChain....418
3007: TcpSTKLoopXbflChain....418
3009: TcpIEBegProfTimer....418
300A: TcpNmiBadRetInfo....419
300B: TCPDvipaError....419
3100: TcpPascalUnexpectCond....419
3101: TcpPascalUnknownFnCode....419
3133: TcpTelnetAbendTrap....419
3134: TcpTelnetStall....419
3202: TcpTestNoNSwap....419
3203: TcpTestSwap....419
3204: TcpTestNoCancel....420
3205: TcpTestCancel....420
3210: TcpTestPSWsuper....420
3211: TcpTestPSWPgm....420
3213: TcpTestPSWUserKey....420
3214: TcpTestPSWSysKey....420
3215: TcpTestPSWBadKey....420
3216: TcpTestAPF1....421
3217: TcpTestAPF0....421
3221: TcpTestTask....421
3222: TcpTestSRB....421
3223: TcpTestJobStep....421
3224: TcpTestTobJob....421
3225: TcpTestAmode24....421

3226: TcpTestAmode31 421
3227: TcpTestAmode64 422
3230: TcpTestSys 422
3231: TcpTestSTC 422
3232: TcpTestInit 422
3233: TcpTestTSO 422
3235: TcpTestOMVS 422
3236: TcpTestAPPC 422
3237: TcpTestUID0 423
C001: TcpJCodeNotValid 423
C009: ResBadReturnInfo 423

Chapter 17. FTPD reply codes 425
125 reply codes 426
125: Appending to data set *name* 426
125 : Appending to named pipe *pathname* 426
125-: Binary tagged file translated with current data connection translation table 427
125: command terminated due to server shutdown in progress 428
125: Could not allocate receive buffer 428
125: Data connection already open; transfer starting 428
125-: Data set access will be retried in 1 minute intervals - *number* attempts remaining 429
125: Data set *dsname* is migrated and NoAutoRecall is specified 430
125: Data set *dsname* is not available 430
125: *dsname* is a physical sequential data set and a member was specified on the RETR command 431
125: DCB *lrecl blksize* 432
125: Error allocating tape data set *dsname* 432
125: Error mounting volume 432
125: Error mounting volume containing data set *dsname* 433
125: error occurred while seeking restart marker 433
125: Error recalling data set *dsname* 433
125: Error recalling data set *data_set* (rc=*rc*) 434
125: File *dsname* not found 434
125: *file_name* request nonexistent member to be sent 434
125-: Format of file number incorrect, *filenum* ignored 435
125-: FTP Server unable to obtain *type* use of *dsname* which is held by: *asid jobname accessmode* on *qname* 435
125: Invalid data set name *"dsname"*. Use MVS Dsname conventions 437
125: JES internal reader *operation* failed 437
125: List started OK for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner* 438
125: List started OK 438
125: List terminated 438
125: Mismatched quotes on pathname *pathname* 439
125: Name length error for pathname *pathname* 439
125: Nlst started OK 439
125: Nlst started OK for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner* 440
125: Non-DASD data set *dsname* cannot be processed 440
125: Open of *dsname* failed 440
125: Retrieve of a whole Partitioned data set is not supported. Use MGET for this purpose 441
125-: Seeking restart marker 441
125: 125 Sending all spool files for requested Jobid 442
125: Sending data set *data set* FIXrecfm *record length* 442
125: Sending data set *name* 442
125: Sending file via NJE to requested destination 443
125: Sending Job to JES internal reader *format record length* 443
125: Storing data in the Null directory (*dev.null) 443
125: Storing data set *name* 444

125: Storing data set *name* (unique name)....444
125: Submit fails: *dsname* User not authorized....444
125-: Submitting job *job_id format record_length*....445
125-: Tagged *type* file translated with table built using file system cp=*codepage_1*, network transfer cp=*codepage_2*....445
125-: Tagged *type* file translated with current data connection translation table....445
125: Transfer aborted: file error....446
125: Transfer aborted: send error....446
125: Transfer request aborted....446
125-: Transferring load module....447
125: Transferring load module....447
125: Unable to get Jobid....447
125: Unable to send *name*....448
125: User Exit refuses this Job to be submitted by *dsname*....448
125: Volume containing *dsname* is not mounted and NoAutoMount specified....448
125: Volume is not ready and automatic tape mounts are not allowed....449
125: VSAM data set *dsname* cannot be processed....449
125: wait ended....450
125-: Waiting for allocation of tape data set *dsname*....450
125-: Waiting for batch pipe subsystem *name* reader to open....450
125-: Waiting for read process to open *pathname*....451
125-: Waiting for recall of data set *data set*....453
125-: Waiting for volume mount for *dsname*....453
125-: Waiting for volume mount for volume *volume*....453
125-: Waiting for write process to open *pathname*....454
125-: Warning TAPEREADSTREAM configured - <NL> in data cannot be translated....455
125: When *job_id* is done, will retrieve its output....455
150 reply codes....455
150: command terminated due to server shutdown in progress....456
150: Waiting for allocation of tape data set *dsname*....456
150: Waiting for recall of data set *dsname*....456
150: Waiting for volume mount for *dsname*....457
200 reply codes....457
200-: Active server dumpIDs -*value_1 value_2 ... value_n*....457
200-: Active server traces - *value_1 value_2 ... value_n*....457
200-: BLOCKSIZE being set to *blksize*....458
200-: BLOCKSIZE must be a multiple of LRECL for RECFM *recfm*....458
200-: BLOCKSIZE must be at least 4 more than LRECL for RECFM *recfm*....459
200-: BLOCKSIZE must equal LRECL for RECFM *recfm*....459
200-: Blocksize parameter *(value)* is not numeric. Blocksize ignored....459
200-: Blocksize parameter *(value)* must be between 0 and 32760. Blocksize ignored....460
200-: BUfno parameter *(value)* is not numeric. BUfno ignored....460
200-: BUfno parameter *(value)* must be between 1 and 255 - BUfno ignored....461
200: BUfno parameter *value* must be from *minimum* to *maximum*. BUfno ignored....461
200 : CCC command successful....461
200-: Chkptint parameter *(value)* is not numeric. Chkptint ignored....462
200-: Chkptint parameter *(value)* is larger than a 4 byte integer. Chkptint ignored....462
200-: Chmod cannot access file *filename* : *error*....462
200-: Chmod failed: *error*....463
200-: Chmod filename is not a valid z/OS UNIX file. CHMOD ignored....463
200-: Chmod invalid filename *filename*....464
200-: Chmod invalid syntax. Specify CHMOD mode filename. CHMOD ignored....464
200-: Chmod mode value invalid. Specify mode as a 1-3 digit octal value, or as {u|g|o|a}{=|+|-}{r|w|x|rw|rx|wx|rwx}. CHMOD ignored....464
200-: Chmod not allowed when user not logged in. CHMOD ignored....465
200-: Chmod parameters missing. Specify CHMOD mode filename. CHMOD ignored....465
200: command terminated due to server shutdown in progress....466
200-: Conddisp parameter *(value)* is invalid. Conddisp ignored....466

200-: Conflicting SITE operands *keyword1* and *keyword2*. *Keyword2* ignored....466
200-: Ctrlconn invalid syntax. Specify CTRLCONN=ascii_code_page_name or CTRLCONN=7BIT. CTRLCONN ignored....467
200 : Data connection protection set to *protection*....467
200-: DATAKEEPALIVE value *value* out of range - value must be 0 or between 60 and 86400 - parameter is ignored....467
200-: Data set "*dsname*" does not exist. Dcbdsn parameter ignored....468
200-: "*dsname*" invalid dsorg. DCBDSN parameter ignored....468
200-: "*dsname*" is a VSAM data set. Dcbdsn parameter ignored....469
200-: "*dsname*" is migrated and noautorecall is specified. DCBDSN parameter ignored....469
200-: "*dsname*" is not on a direct access volume. Dcbdsn parameter ignored....470
200-: Data set name missing from DCBDSN parameter. DCBDSN parameter ignored....470
200: Data transfer is mixed SBCS/DBCS....470
200: Data transfer is pure DBCS....471
200: Data transfer mode is *type*....471
200-: Dataclass parameter *(value)* is more than 8 characters. Dataclass ignored....471
200-: DB2 parameter *(db2name)* is more than 4 characters. DB2 ignored....472
200-: Debug values not supported :*value_1 value_2 ... value_n*....472
200-: Dest node longer than 8 characters. Dest ignored....473
200-: Dest user longer than 8 characters. Dest ignored....473
200-: Destination *(value)* is more than 8 characters. Dest ignored....473
200-: Directory parameter *(value)* is not numeric. Directory ignored....474
200-: Directory parameter *(value)* must be between 1 and 16777215. Directory ignored....474
200-: Dump values not supported -*value_1 value_2 ... value_n*....474
200: EPRT request OK....475
200: EPSV ALL accepted....475
200-: Error locating file "*dsname*". DCBDSN parameter ignored....475
200-: Error mounting "*dsname*". DCBDSN parameter ignored....476
200-: Error retrieving "*dsname*". DCBDSN parameter ignored....476
200-: Filename for Xlate parameter (*name*) exceeds maximum length of *length*. Xlate ignored...477
200-: Filetype parameter *(value)* is invalid. Filetype ignored....477
200-: Ignoring *parameter*. The keyword was already specified on this SITE command....477
200-: Ignoring *parameter=value*. The keyword was already specified on this SITE command....478
200-: Invalid format data set name "*name*". Dcbdsn parameter ignored....478
200-: Invalid record format '*value*' encountered....479
200-: JESINTERFACELEVEL=*value*. The value of *keyword* cannot be modified....479
200-: Jeslrecl parameter *(value)* is not numeric. Jeslrecl ignored....479
200-: JesLrecl parameter must be between 1 and 254. JesLrecl parameter ignored....480
200-: Jesrecfm parameter *(parameter)* is invalid. Jesrecfm ignored....480
200-: *keyword=value* ignored. Unable to set up requested conversion....480
200: Language is en-US (United States English)....481
200- : Language reverts to default en-US (United States English)....481
200: Load module transfer reset....482
200: Local byte size is 8, representation type is Image....482
200-: LRECL being changed to *lrecl*....482
200-: LRECL being reset to *lrecl*....483
200-: LRECL being reset to SITE default of 'not used'....483
200-: Lrecl parameter *(value)* is not numeric. Lrecl ignored....483
200-: Lrecl parameter *(value)* must be between 0 and 32760. Lrecl ignored....484
200-: LRECL X valid only for RECFM of U or variable length spanned....484
200-: LRECL 0 valid only for RECFM of U....485
200-: LRECL, RECFM, and BLOCKSIZE being reset to default values....485
200-: Mgmtclass parameter *(value)* is more than 8 characters. Mgmtclass ignored....485
200-: Migratevol parameter *(value)* is more than 6 characters. Migratevol ignored....486
200-: NCP parameter not supported for the C server. NCP ignored....486
200-: No conversion available to *'cp_name1'* from *'cp_name2'*. MBDATACONN ignored....487
200-: No conversion available between *parm1* and *parm2*. SBDATACONN ignored....487
200-: No storage volumes exist....487

200-: No users are allowed to use SITE DEBUG....488
200-: No users are allowed to use SITE DUMP....488
200-: Nowrtapefastio ignored. Wrtapefastio already specified on this Site command. 488
200: OK....489
200-: Operand not allowed on *parm* parameter. Parameter ignored....489
200-: operand required on *parm* parameter. Parameter ignored....490
200-: Parameter *keyword* value *value* is not numeric - the parameter is ignored....490
200-: Parameter *parameter* value *value* must be in the range *minimum* to *maximum* - parameter is ignored....491
200-: *parameter=operand* ignored. Requested conversion is not supported....492
200 : PBSZ=0 is the protection buffer size....492
200 : PBSZ=*size*....492
200-: Percent Free Free Largest Free 493
200: Port request OK....494
200-: Primary parameter *(value)* is not numeric. Primary ignored....494
200-: Primary parameter *(value)* must be between 1 and 16777215. Primary ignored....494
200 : Protection buffer size accepted....495
200-: Qdisk ignored. "*value*" is not a valid volser....495
200-: Qdisk workarea allocation failed....495
200-: READTAPEFormat *value* is not supported - READTAPEFormat ignored 496
200-: Recfm parameter *(value)* is invalid. Recfm ignored....496
200-: Representation type is Big5....496
200: Representation type is Ebcdic IBM Kanji....497
200: Representation type is Image....497
200-: Representation type is SChinese....497
200: Representation type is *type*....498
200: Representation type is UCS-2....498
200-: Retpd parameter *(value)* is not numeric. Retpd ignored....498
200-: Retpd parameter *(value)* must be between 0 and 9999. Retpd ignored....499
200-: Sbdataconn invalid syntax. Specify SBDATACONN=(value1,value2) or SBDATACONN=dsn. SBDATACONN ignored....499
200-: Sbdataconn parameter is too long. Maximum length for code page name is *length*. SBDATACONN ignored....500
200-: SBSUBChar parameter (*sbsubchar*) is not valid - SBSUBChar ignored....500
200-: Secondary parameter *(value)* is not numeric. Secondary ignored....500
200-: Secondary parameter *(value)* must be between 0 and 16777215. Secondary ignored....501
200: SITE command was accepted....501
200-: Some characters cannot be translated between *codeset_1* and *codeset_2*....502
200-: SO/SI characters *char* used....502
200-: Sqlcol parameter *(value)* is invalid. Sqlcol ignored....502
200: Standard DBCS control used....503
200-: Storclass parameter *(value)* is more than 8 characters. Storclass ignored....503
200-: SUBSYS parameter *(value)* is more than 4 characters - SUBSYS parameter is ignored....504
200-: The keyword *keyword* value of *value* is not valid. Parameter ignored....505
200: Transferring PDS directory information....505
200-: Translate file '*file*' invalid. SBDATACONN ignored....505
200-: Translate file '*file*' not found. SBDATACONN ignored....506
200-: Translate file for Xlate name '*name*' not found. Xlate ignored....506
200-: Translate file for Xlate name '*name*' not valid. Xlate ignored....507
200-: UCOUNT parameter *(value)* is neither numeric, nor P. UCOUNT ignored....507
200-: UCOUNT parameter *(value)* must be between 1 and 59, or P. UCOUNT ignored....507
200-: Umask invalid syntax. Specify UMASK umask_value. UMASK ignored....508
200-: Umask value invalid. Specify Umask value as 1 - 3 octal digits....508
200-: Umask value missing. Specify Umask value as 1 - 3 octal digits....509
200-: Unable to set up conversion between '*parm1*' and '*parm2*'. SBDATACONN ignored....509
200-: Unable to set up conversion between UCS-2 and *codeset*....509
200-: Unit ignored. "*value*" is not a valid unit parameter....510
200-: Unrecognized parameter '*parameter=operand*' on SITE command....510

200-: Unrecognized parameter '*parameter*' on SITE command.... 511
200-: User *userid* is not authorized to filter on *keyword*. Its value remains *value*.... 511
200-: User *user_name* is not allowed to use SITE DEBUG.... 511
200-: User *user_name* is not allowed to use SITE DUMP.... 512
200-: VCOUNT parameter is not numeric. VCOUNT ignored.... 512
200-: VCOUNT parameter must be between 1 and 255. VCOUNT ignored.... 513
200-: volume for "*dsname*" is not mounted and noautomount is specified. DCBDSN parameter ignored.... 513
200-: Volume Free Cyls Trks Cyls-Trks Exts Use Attr.... 513
200-: Volume ignored. "*value*" is not a valid volume parameter.... 514
200-: *volume percent_free free_cylinders free_tracks largest_cyls largest_trks free_extents use_attribute*.... 515
200-: Volume *volser* could not be found.... 516
200-: Waiting for mount for "*dsname*".... 516
200-: Waiting for recall of "*dsname*".... 516
200-: Wrtapefastio ignored. Nowrtapefastio already specified on this Site command. 517
200-: Xlate parameter (*xlate_name*) is more than 8 characters. Xlate ignored.... 517
202 reply codes.... 517
202: ACCT command not required - ignored.... 518
202: ALLO not necessary, you may proceed.... 518
202: command terminated due to server shutdown in progress.... 518
202: SITE not necessary; you may proceed.... 519
205 reply codes.... 519
205: Load module transfer syntax error.... 519
205: Load module transfer syntax error: blksize parameter missing.... 519
205: Load module transfer syntax error: lrecl parameter missing.... 520
211 reply codes.... 520
211: command terminated due to server shutdown in progress.... 520
211-: Confidence level in data transfers is neither checked nor reported.... 520
211-: Confidence level in data transfers is checked and reported.... 521
211-: Confidence level in data transfers is not checked or reported.... 521
211-: DBSUB is set to *dbsub*.... 522
211: End.... 522
211-: Extensions supported.... 523
211-: ISPFSTATS is set to *ispfstats*.... 523
211: no Extensions supported.... 523
211-: Outbound MBCS ASCII data uses *lt_chars* line terminator.... 524
211-: Outbound SBCS ASCII data uses *lt_chars* line terminator.... 524
211-: Partitioned data sets will be created in extended format.... 525
211-: Records on input tape are fixed format.... 525
211-: Records on input tape are lrecl X format.... 526
211-: Records on input tape are spanned format.... 526
211-: Records on input tape are unspecified format.... 526
211-: Records on input tape are variable format.... 527
211-: SBSUBCHAR is set to *sbsubchar*.... 527
211-: SBSUB is set to *sbsub*.... 528
211-: Server site variable *statement_name* is set to *value*.... 528
211-: Timer *timer_name* is set to *timer_value*.... 529
211: The value of option *option* is undefined.... 529
211: TLS security is supported at the *tlsRfcLevel* level.... 529
211-: UTF-8 encoding in use on the control connection.... 530
213 reply codes.... 530
213: command terminated due to server shutdown in progress.... 531
213: Status: *number* bytes transferred.... 531
213: YYYYMMDDHHMMSS.... 531
214 reply codes.... 532
214: command terminated due to server shutdown in progress.... 532
214: XDSS *dsname*: extract the attributes of an MVS data set.... 532

214-: READTAPEFormat=value Format of input tape data sets. Valid formats are 533
214-: F (for fixed), V (for variable), S (for spanned), ... 533
214-: X (for lrecl X), and blank (unspecified). 533
215 reply codes..... 533
215: command terminated due to server shutdown in progress..... 533
215: MVS is the operating system of this server. FTP Server is running on *name*..... 533
215: UNIX is the operating system of this server. FTP Server is running on *name*..... 534
220 reply codes..... 534
220: command terminated due to server shutdown in progress..... 534
220: Connection will close if idle for more than *timeout*..... 535
220: Connection will not timeout..... 535
220-: FTP *init_time* on *init_date*. 535
220-: *jobname* IBM FTP *version_release* at *hostname*, *init_time* on *init_date*..... 536
220: Reinitialized; Ready for new user..... 536
220-: The message was truncated..... 536
221 reply codes..... 537
221: command terminated due to server shutdown in progress..... 537
221: Quit command received. Goodbye..... 537
226 reply codes..... 537
226: Abort successful..... 537
226: command terminated due to server shutdown in progress..... 538
226-: Compression reduced bytes transferred by *percentage* percent 538
226-: DBCS conversion to EBCDIC encountered invalid input (*number* errors)..... 539
226-: It is known to JES as *job_ID*..... 539
226: List completed successfully. 539
226: Nlst completed successfully 540
226-: One or more characters were substituted during the transfer 540
226: Statistics have been updated for the PDS member that was transferred 541
226: Transfer completed (data was truncated) 541
226: Transfer completed (lines were wrapped)..... 541
226: Transfer completed (*number* translation errors) 542
226: Transfer completed successfully..... 542
226: Transfer completed successfully, warning SELECT file too large..... 542
226-: Unicode to EBCDIC conversion resulted in *number* substitutions 543
227 reply codes..... 543
227: command terminated due to server shutdown in progress..... 543
227: Entering Passive Mode *(h1,h2,h3,h4,p1,p2)*..... 544
229 reply codes..... 544
229: Entering Extended Passive Mode (|||*port_number*|)..... 544
230 reply codes..... 544
230: command terminated due to server shutdown in progress..... 544
230-: Password was changed..... 545
230-: Processing FTPS.RC configuration file - *filename* 545
230: The email address entered is in an incorrect format..... 546
230-: The message was truncated..... 546
230-: Unable to open FTPS.RC configuration file - *filename* - *errno* 546
230-: Unrecognized command - *cmd* - entered 547
230: *user_id* is logged on. Working directory is "*directory*"..... 547
230-: User *userid* is an authorized user..... 547
230-: Unrecognized parameter '*parameter=operand*'on SITE command..... 548
234 reply codes..... 548
234 : Security environment established - ready for negotiation..... 548
235 reply codes..... 549
235 : ADAT=*base64EncodedData*..... 549
235 : GSSAPI Authentication succeeded..... 549
250 reply codes..... 549
250: Cancel successful..... 549
250: command terminated due to server shutdown in progress..... 550

250-: Compression reduced bytes transferred by *percentage* percent ... 550
250: *dsname* deleted ... 550
250: *dsname* deleted from migration volume ... 551
250: Data structure is File ... 551
250: Data structure is Record ... 551
250-: DBCS conversion to EBCDIC encountered invalid input (*number* errors) ... 552
250: DCB saved, send next command for load module transfer ... 552
250: "*directory*" is the working directory name prefix ... 552
250: directory remains "*old_directory*" ... 553
250-: Error mounting "*dsname*"; ... 553
250-: Error retrieving "*dsname*"; ... 553
250: z/OS UNIX directory *directory* is the current working directory ... 554
250-: It is known to JES as *job_ID* ... 554
250-: JES SSI interface return code *rc* ... 555
250-: JESENTRYLIMIT of *number* reached. Additional entries not displayed ... 555
250-: JES SSI function *function* SSOBRETN = *rc* ... 555
250: List completed successfully ... 556
250: Nlst completed successfully ... 556
250: *old data set* renamed to *new data set* ... 556
250-: One or more characters were substituted during the transfer ... 557
250: Rename requested and the new name is the same as the old ... 557
250-: Statistics have been updated for the PDS member that was transferred ... 557
250-: The message was truncated ... 558
250: The working directory "*directory*" is a partitioned data set ... 558
250-: The working directory might be a load library ... 558
250: Transfer completed (data was truncated) ... 559
250: Transfer completed (lines were wrapped) ... 559
250: Transfer completed (*number* translation errors) ... 560
250: Transfer completed successfully ... 560
250: Transfer completed successfully, warning SELECT file too large ... 560
250: *type size* - send next command for load module transfer ... 561
250-: Unicode to EBCDIC conversion resulted in *number* substitutions ... 561
250-: Waiting for mount for "*dsname*" ... 561
250-: Waiting for recall of "*dsname*" ... 562
250-: Working Directory for PUT is NULL Device; ... 562
250: for GET is "*directory*" partitioned data set ... 562
250-: Working Directory for PUT is NULL Device; ... 563
250: for GET is z/OS UNIX directory *directory* ... 563
250-: Working Directory for PUT is NULL Device; ... 563
250: for GET is "*directory*" name prefix ... 563
251 reply codes ... 563
251: Current working directory is not a PDS ... 564
251: Current working directory is not a PDSE ... 564
252 reply codes ... 564
252: Current working directory is not a load library ... 564
252: No load module transfer processing necessary ... 565
253 reply codes ... 565
253: Could not build a file list ... 565
253: No members of the data set match the selection pathnames ... 565
254 reply codes ... 566
254: Load module transfer requires filetype=SEQ ... 566
257 reply codes ... 566
257: command terminated due to server shutdown in progress ... 566
257: "'*directory*'" created ... 567
257: "*directory*" is the z/OS UNIX working directory ... 567
257: "'*directory*'" is working directory ... 567
257: "'*directory*'" partitioned data set is working directory ... 568
257: MKD failed. Error mounting volume ... 568

257: named pipe *pathname* created.... 568
257-: Waiting for volume mount for volume *volume*....569
257-: Working Directory for PUT is NULL Device;.... 569
257: for GET is "*directory*" partitioned data set....569
257-: Working Directory for PUT is NULL Device;.... 570
257: for GET is z/OS UNIX directory *directory*.... 570
257-: Working Directory for PUT is NULL Device;.... 570
257: for GET is "*directory*" name prefix.... 570
300 reply codes.... 570
300: command terminated due to server shutdown in progress.... 571
300: Restart command accepted, parameter *restart checkpoint*....571
331 reply codes.... 571
331: command terminated due to server shutdown in progress.... 571
331: Send email address as password please.... 572
331: Send password please....572
334 reply codes.... 572
334: Using authentication mechanism *mechanism*....572
335 reply codes.... 573
335 : ADAT=*base64EncodedData*.... 573
335 : More data needed....573
350 reply codes.... 573
350: command terminated due to server shutdown in progress.... 574
350: REST command accepted, parameter *byte_transfer_offset*....574
350: RNFR accepted. Please supply new name for RNTO....574
400 reply codes.... 575
400: command terminated due to server shutdown in progress.... 575
421 reply codes.... 575
421: command terminated due to server shutdown in progress.... 575
421: connection terminated - setuid failure during REIN command processing. *error*....576
421: Open rejected due to insufficient resources....576
421: User Exit rejects open for connection.... 576
425 reply codes.... 577
425: Can't open data connection....577
425: Can't open passive connection....577
425: command terminated due to server shutdown in progress.... 578
425-: Server requires protected data connection....578
425: Unable to open data connection.... 578
426 reply codes.... 579
426: command terminated due to server shutdown in progress.... 579
426: Connection closed; transfer aborted.... 579
426: Data connection aborted....579
426-: Data set *dsname* is allocated to another job and is unavailable for *cmd* command....580
450 reply codes.... 580
450: command terminated due to server shutdown in progress.... 580
450: Data set *dsname* is allocated to another job and is unavailable for *cmd* command.... 581
450: JESGET failed, could not allocate send buffer....581
450-: Record too long.... 581
450: timer expired waiting for read process to open *pathname*.... 582
450: timer expired waiting for write process to open *pathname*.... 583
450: timer expired while reading from named pipe....584
450: Cannot create unique data set name for store unique of dsname....585
451 reply codes.... 586
451-: Checkpoint marker not supported....586
451: command terminated due to server shutdown in progress.... 586
451-: Compression reduced bytes transferred by *percentage* percent.... 586
451-: Data set is full (19)....587
451-: Data set is full *rc*....587
451-: Data set is out of space....587

451: data transfer aborted - command terminated due to CPU time limit exceeded..... 588
451: data transfer aborted - command terminated due to server shutdown in progress..... 588
451: Dele failed due to internal error..... 589
451: Dele failed, too many entries..... 589
451-: Device is out of space..... 589
451: Error (*error*) closing the data set..... 590
451: Error (*error*) closing the data set. File could not be deleted..... 590
451: Error (*error*) closing the data set. File is catalogued..... 590
451: Error (*error*) closing the data set. File is deleted..... 591
451: Error *(rc)* closing the data set *dsname*..... 591
451-: File transfer failed. File contains records that are longer than the LRECL of the new file..... 591
451: File transfer failed. Multi-byte data conversion error occurred..... 592
451: File Transfer might not be complete. Last record received without EOL sequence..... 592
451: Index *index* is greater than number of spool files for *jobid*..... 593
451: Internal storage allocation error, JesPutGet aborted..... 593
451: Internal storage allocation error, try again later..... 593
451: JESGET aborted: internal error processing JES request..... 594
451: JESPUTGET aborted: internal error processing JES request..... 594
451: List failed due to internal error..... 594
451: List failed, too many entries..... 595
451-: LRECL *lrecl* is incompatible with RECFM *recfm*..... 595
451: Nlst failed due to internal error..... 595
451: Nlst failed, too many entries..... 596
451-: Possible cause is the destination PDS or its directory is too small..... 596
451-: Record is too long to process..... 596
451-: Record received was too short (4)..... 597
451: Renaming attempt failed..... 597
451-: System completion code and reason: *cc-rc*..... 598
451: Transfer aborted..... 598
451: Transfer aborted due to file error..... 598
451: Transfer aborted due to file error. File could not be deleted..... 599
451: Transfer aborted due to file error. File is catalogued..... 599
451: Transfer aborted due to file error. File is deleted..... 599
451: Transfer aborted due to receive error..... 600
451: Transfer aborted due to receive error. File could not be deleted..... 600
451: Transfer aborted due to receive error. File is catalogued..... 600
451: Transfer aborted due to receive error. File is deleted..... 601
451: Transfer aborted. File could not be deleted..... 601
451: Transfer aborted. File is catalogued..... 602
451: Transfer aborted. File is deleted..... 602
451: Transfer aborted: file error..... 602
451: Transfer aborted: internal error while processing SQL request..... 603
451: Transfer aborted: send error..... 603
451: Transfer aborted: SQL FETCH error *(code)*..... 603
451: Transfer completed..... 604
451-: Unable to get Jobid..... 604
451: Unrecoverable error from JES SSI request RC=*rc*..... 604
452 reply codes..... 605
452: command terminated due to server shutdown in progress..... 605
452: insufficient storage to process SITE command..... 605
452: Transfer aborted: insufficient storage to process SQL request..... 605
500 reply codes..... 606
500: Command failed - command too long..... 606
500: command terminated due to server shutdown in progress..... 606
500: Invalid restart parameter..... 607
500: unknown command *command*..... 607
500: User Exit denies user from using Command '*command*'..... 607
500: User Exit denies Userid '*user_ID*' from using Command '*command*'..... 608

500-: UX-*explanation*....608
501 reply codes....608
501: * is not last char....609
501: ** must be preceded and followed by a period or blank....609
501: A qualifier in "*pathname*" begins with an invalid character....609
501: A qualifier in "*pathname*" is more than 8 characters....610
501: A qualifier in "*pathname*" contains an invalid character....610
501 : Base 64 decode failed for ADAT data: *error*....610
501 : Base 64 decode failed for *command* command: *error*....611
501: command aborted - error in local processing....612
501: command aborted -- FTP server not configured for *commandname*....612
501: command *command* fails: "" is not a valid directory name....612
501: *command* command syntax error : too many parameters....613
501: command OPTS aborted -- no options supported for *command*....613
501: *command* supported only in Stream mode....613
501: command terminated due to server shutdown in progress....614
501: CWD ../ only valid for z/OS UNIX directories....614
501: Data set name too long. Use MVS naming conventions....614
501: Data set name too long. Use MVS or z/OS UNIX data set naming conventions....615
501: '*data_set(member)*' requests members but *data_set* is not a partitioned data set....615
501: Directory is already NULL....616
501: Error - existing kanji type invalid....616
501: Error - existing type invalid....616
501: Error - existing UCS type invalid....617
501: File name too long. Use z/OS UNIX file naming conventions....617
501: Invalid data set name *"dsname"*. Use MVS Dsname conventions....617
501: Invalid data set name. Use MVS Dsname conventions....618
501: Invalid directory name - too large....618
501: Invalid file identifier in RNTO command....619
501: Invalid Jobid....619
501: Invalid user name '*' in USER command....619
501: Member name too long. Use MVS naming conventions....620
501: Mismatched quotes on directory name "*pathname*"....620
501: MKDIR fails: *reason*....620
501: No directory name entered....621
501: Nonexistent GDG data set *dsname*....621
501: One or more parameters missing from command *command*....621
501: Partitioned data set may not be created within a partitioned data set....622
501: Partitioned data set may not be deleted within a partitioned data set....622
501: password missing from PASS command....623
501: Pathname required with null working directory....623
501: Patterns (% and *) may only be specified in the last qualifier when in directory mode....623
501: Protection buffer size value is not valid....624
501: Qualifier too long. Use MVS naming conventions....624
501: RMDIR fails: *reason*....624
501: Store unique not supported for GDG data sets....625
501: syntax error -- command required for OPTS....625
501: Syntax error -- marker required for REST....625
501: syntax error -- pathname *pathname* not allowed for working directory *directory*....626
501: syntax error -- pathname required for *command*....627
501: too many bad passwords entered, PASS command disabled....627
501: TYPE command contains invalid parameter....628
501: TYPE command syntax error: *num* parameter invalid....628
501: TYPE command syntax error: *reason*....628
501: Type remains *type*....629
501-: Unknown mode *new_mode*....629
501: Data transfer mode remains *old_mode*....629
501-: Unknown structure *new_stru*....630

501: Data structure remains *old_stru*....630
501-: unknown type *type_value*....630
501: User name missing from USER command....630
501: Wildcards not allowed in PDS name....631
502 reply codes....631
502: command aborted -- server not configured for LANG....631
502: command aborted -- UTF-8 translation not available....631
502: command *command* not implemented....632
502: command terminated due to server shutdown in progress....632
502: error in host address....633
502: error in host address '*value*'....633
502: error in port number....634
502: error in port number '*value*'....634
502: error parsing *command_name* command....635
502: PORT command syntax error - insufficient digits in host-port....635
503 reply codes....635
503 : Authentication already established....636
503: Command *command* rejected - *command* not allowed after *prior_command* command....636
503: command terminated due to server shutdown in progress....637
503: EPSV ALL received - *command* not allowed after EPSV ALL....637
503 : Must first establish authentication....637
503 : Must first issue PBSZ....638
503 : Must issue AUTH command before ADAT command....638
503: PASS command must be preceded by USER....639
503 : Server on the TLS secure port does not accept the AUTH command....639
504 reply codes....639
504: Block mode not implemented for type B....639
504: Command *command* aborted -- FTP server not configured for parameter *parameter*....640
504: command *command* into named pipe fails -- filetype must be SEQ....640
504: command STOU not supported for named pipes....641
504: command terminated due to server shutdown in progress....642
504: Compress mode not implemented for type B....642
504: Data structure remains *old_stru*....643
504: Error - existing kanji type invalid....643
504: Error - existing type invalid....644
504: Filetype SQL requires type A (ASCII) or E (EBCDIC) or B (DBCS)....644
504: Lrecl X transfer not supported with *condition*....644
504: Lrecl X transfer not supported with Record I/O....645
504: NOASATRANS is not supported for TYPE U. Use 'SITE ASATRANS'....645
504: Only local byte size allowed is 8....645
504-: Only 'TYPE U 2' is supported....646
504-: Page structure not implemented....646
504: parameter *parameter* not supported....646
504: Port command not implemented for that parameter....647
504: Record structure is not supported for TYPE U transfer....647
504: Restart not allowed for named pipes....648
504 : Restart not allowed with active security mechanism....648
504: restart is not supported for type *type*....649
504: Restart not allowed for store unique....649
504: Restart requires Block or Compressed transfer mode....649
504: Restart requires EBCDIC data type....650
504: Restart requires filetype=SEQ....650
504 : Server does not understand the specified mechanism....650
504 : Server does not understand the specified protection level....651
504: Server SBSENDEOL must be CRLF for SIZE command....651
504: Server SBSENDEOL must be CRLF for stream mode restart of RETR command....652
504: STAT file-identifier: not implemented....653
504: Stream mode restart not supported for MVS data sets....653

504: Struct R implemented with stream mode only.... 653
504: SUBSYS parameter not supported for APPE command 654
504: Transfer of RDWs is not supported for TYPE U. Use 'SITE NORDW'.... 655
504: Transfer of trailingblanks is not supported for TYPE U. Use 'SITE NOTRAILINGBLANKS'.... 655
504-: TYPE command contains extraneous parameter *parm*.... 655
504: Type *format* file transfer is not supported when SUBSYS is configured.... 656
504-: TYPE has unknown format *format*.... 657
504-: TYPE has unsupported format *format*.... 657
504-: TYPE not Supported. Translation table not Loaded.... 657
504-: Type not supported. Unable to load *lang* translation tables.... 658
504: Type remains *type*.... 658
504: TYPE U transfer is not supported for filetype *type*.... 658
504: TYPE U transfer is not supported in mode *mode*.... 659
504: TYPE U transfer is supported only for filetype SEQ.... 659
504: TYPE U transfer is supported only in stream mode.... 659
504-: Unable to set up conversion between UCS-2 and *codeset*.... 660
504 : Unknown authentication type *mechname*.... 660
504: WRAPRECORD is not supported for TYPE U. Use 'SITE NOWRAPRECORD'.... 661
509 reply codes.... 661
509: cannot convert pathname to native character set.... 661
521 reply codes.... 661
521: command terminated due to server shutdown in progress.... 661
521: *“new_directory”* data set already exists.... 662
522 reply codes.... 662
522: command PORT not allowed with this session - current protocol is not IPv4. 662
522: network protocol *netprt_specified* not consistent with this session. Use *netprt_allowed*.... 663
522: Network protocol not supported. Use (*supported_protocols*).... 664
522: No IPv4 address available for PASV. Use EPSV.... 664
525 reply codes.... 665
525: No data is available on the data connection.... 665
530 reply codes.... 665
530-: A load was done from an uncontrolled library.... 665
530-: An error occurred in the security product.... 666
530-: An MVS environmental or internal error occurred.... 666
530-: Anonymous login with security protected session requires anonymousLevel > 2.... 666
530: Closing control connection.... 667
530: command terminated due to server shutdown in progress.... 667
530-: Current user *current user* remains logged in.... 668
530-: email address rejected by user exit.... 668
530-: Error on *func* function call, errno=*errno*, rsncode=*errnojr*.... 668
530-: error processing PASS command : *error*.... 669
530: Excessive bad passwords entered - USER command disabled.... 669
530-: Initial filetype *file_type* is disabled for anonymous.... 670
530-: Internal processing error.... 670
530: Login attempt by *user ID* rejected by user exit.... 670
530: Logon attempt by '*user_id*' rejected.... 671
530: new password format invalid.... 671
530: new passwords are not the same.... 671
530: Not logged in.... 672
530-: Number of groups exceeds the maximum number allowed.... 672
530: PASS command failed.... 673
530: PASS command failed - getpwnam() error : *error*.... 673
530: PASS command failed - _passwd() error : *error*.... 673
530-: Password was changed.... 674
530-: Process does not have permission to set the UID.... 674
530 : Server requires authentication.... 674
530 : Server requires authorized user.... 675
530-: StartDirectory *value* is disabled for anonymous.... 675

530-: System authorization facility (SAF) had an error....676
530-: The caller is not authorized....676
530-: The email address entered is in an incorrect format....676
530-: The newpass is not valid....677
530-: The old password has expired....677
530-: The old password is not authorized....677
530-: The password is not authorized....678
530-: The process is currently not able to change UID....678
530-: The username access was denied by SAF services....678
530-: The username is unknown....679
530-: The username, oldpass or newpass argument is invalid....679
530-: The value of uid is incorrect....680
530: USER command failed....680
530-: USER command failed. Switch from *current user* to *new user* not accepted....680
530-: User *userid* is not allowed to access server's port....681
530: You must first login with USER and PASS....681
531 reply codes....681
531 : Server requires client certificate for login processing....681
532 reply codes....682
532 : Username does not match name in client certificate....682
533 reply codes....682
533 : All commands must be ENC protected....682
533 : All commands must be protected....683
534 reply codes....683
534 : CCC not supported....683
534: Command *command* not allowed for connection to secure port....684
534: Could not stop TLS security....684
534 : Server does not support the ADAT command for TLS secured connection....685
534 : Server does not turn off protection for TLS secured control connection....685
534 : Server is not willing to accept security mechanism....686
534: Server is not willing to accept security mechanism on this connection....686
534 : Server is protected and is not willing to accept another AUTH command....687
534 : Server requires authentication before command processing....687
534 : Server requires authentication before PASS command....687
534 : Server requires authentication before USER command....688
534 : Server setup for TLS failed....688
534: TLS negotiation failed -- data connection closed....688
535 reply codes....689
535: Attempt to decrypt data failed....689
535: Attempt to encrypt data failed....689
535-: GSSAPI error major status code: *value - text*....690
535-: GSSAPI error minor status code: *value - text*....690
535 : Length *length* of received buffer is greater than PBSZ *size*....690
535 : Request to accept security context failed....691
535 : Request to acquire security credentials failed....691
535 : Request to import name failed....692
535 : Request to import the security context failed....692
535: Request to load the Kerberos DLL library failed....692
536 reply codes....693
536 : Data connection protection *level* not supported....693
550 reply codes....694
550: Allocation for remote destination failed....694
550: Allocation of *dsname* failed while executing *command* command....694
550: Allocation of *dsname* failed while executing *cmd* command....694
550: Allocation of *data_set* failed: (rc=*rc*, err=*err*, info=*info*)....695
550: Allocation of temporary data set failed: (rc=*rc*, err=*err*, info=*info*)....695
550-: anonymous login rejected by FTP server....696
550 : command *command* fails: *message_prefix reason* (errno2 = *errno2*)....696

550: command *command* fails - unable to create named pipe *pathname*.... 697
550: command *command* into *pathname* not supported when UNIXFILETYPE is FIFO....698
550: Cannot create unique data set name for store unique of *dsname*.... 699
550: Cannot create unique file name for store unique of *filename*.... 699
550: Cannot create unique member name for append to *dsname*.... 700
550: Cannot create unique member name for store unique of *dsname*.... 700
550: cannot determine characteristics of *pathname*....700
550: Cannot rename from partitioned data set *dsname* to a different partitioned data set *dsname*....701
550: closing control connection.... 701
550: *cmd* cmd failed : *error*....702
550: *cmd* cmd failed. No files found....702
550: *cmd* command failed - popen error: *error*....702
550: *cmd* failed. Unknown HOME directory.... 703
550: *cmd* fails: *dsname*. User not authorized.... 703
550: *cmd* fails: *filename* is a directory and is not empty....703
550: *cmd* fails: *pathname* is a directory.... 704
550: *cmd* fails: *pathname* is not a directory.... 704
550: Command *command* fails: access to resource is denied by server.... 704
550: Command *cmd* failed - pipe error: *error*.... 706
550: command *cmd* fails: *filename* does not exist....706
550: Command *cmd* fails: *filename* is a character special file....706
550: Command *cmd* fails: *filename* is an unknown type.... 707
550: Command *cmd* fails: *filename* is a directory.... 707
550: Command *cmd* fails: *filename* is a pipe or FIFO.... 707
550: command *command* fails: filetype is *file type*....708
550: Command *cmd* fails - *name* is of an unsupported type....708
550: command *command* fails - *pathname* must be an MVS directory.... 709
550 : command *command* fails: *pathname* - user is not authorized....710
550: command *command* is not available for *pathname*.... 711
550: command *command* is not supported for mode *mode*.... 711
550: command *command* is not supported for structure *structure*.... 712
550: command *command* is not supported for type *type*....712
550-: command *command* rejected - file transferred while SBSENDEOL not CRLF....712
550: *command* fails: *dsname*. User not authorized.... 713
550: *command* fails: *pathname*. User not authorized....713
550: command SIZE is not supported for the current data connection translate table when type is *type*.... 714
550: command SIZE rejected - *pathname* contains CR characters.... 714
550: command SIZE rejected - *pathname* is not an z/OS UNIX file....714
550: Command terminated due to CPU time limit exceeded....715
550: command terminated due to server shutdown in progress.... 715
550: could not delete *dataset*....716
550: Data set *dsname* is migrated and NoAutoRecall is specified....716
550: Data set *dsname* not found.... 717
550: "*directory*" data set does not exist....717
550: *dsname* is a partitioned data set and no member was specified on the *cmd* command..... 718
550: *dsname* is a physical sequential data set and a member was specified on the command.....718
550: *dsname* is not on a direct access volume. It may not be deleted.... 718
550: *dsname* is not on a direct access volume. It may not be renamed....719
550: *dsname* used exclusively by someone else.... 719
550: DELE fails: *dsname* does not exist.... 719
550: DELE fails: *dsname*. User not authorized....720
550: directory remains "*file_name*".... 720
550: DSORG=DA requires structure: FILE, mode: STREAM, and transfer type: IMAGE....720
550: error allocating *new_directory*....721
550: Error allocating storage for *type*....721
550: Error allocating tape data set *dsname*....721

550: Error deleting migrated data set *dsname*.... 722
550-: error initializing FTP server.... 722
550: Error mounting volume containing data set *dsname*.... 723
550: Error opening *data_set_name*.... 723
550: error reading PDS directory.... 723
550: Error recalling data set *data_set*.... 724
550: Error recalling data set *data_set* (rc=*rc*).... 724
550: File *filename* not found.... 724
550: *file_name* requests a nonexistent partitioned data set. Use MKD command to create it.... 725
550-: GSSAPI error major status code: *value* - *text*.... 725
550-: GSSAPI error minor status code: *value* - *text*.... 725
550: Index *number* is greater than number of spool files for *jobid*.... 726
550: internal error processing *command* command.... 726
550-: Internal error processing *function* SSOBRETN=*rc*.... 727
550: Invalid cancel request.... 727
550: Invalid jobname/Jobid combination.... 727
550: JES cannot find output for *jobid*.... 728
550: JES cannot find output for *jobid*, JesPutGet aborted.... 728
550: JES internal reader allocation failed.... 728
550: JES internal reader open failed.... 729
550: JES is unable to provide spool data set name now.... 729
550: JES is unable to provide spool data set name now, JesPutGet aborted.... 729
550: JES spool file allocation failed for *dsname*.... 730
550: JES spool file open failed for *dsname*.... 730
550: JESPUT failed, could not allocate receive buffer.... 730
550: JesPutGet aborted.... 731
550: JesPutGet aborted, internal error.... 731
550: JesPutGet aborted, job not found.... 731
550: JesPutGet aborted, timeout exceeded.... 732
550: JesPutGet terminated.... 732
550: Job name not found.... 732
550: Job not cancelled, duplicate jobnames and no Jobid.... 733
550: Job not cancelled, job on output queue.... 733
550: Jobid *jobid* not found.... 733
550: Jobid *jobid* not found for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner*.... 734
550: Jobid with invalid syntax for subsystem.... 734
550: Mismatched quotes on pathname *pathname*.... 735
550: MKD failed. Dcbdsn data set *dcbdsn_name* does not exist.... 735
550: MKD failed. Dcbdsn data set *dcbdsn_name* is not on a direct access volume.... 735
550: MKD failed. Dcbdsn data set *dcbdsn_name* is a VSAM data set.... 736
550: MKD failed. Dcbdsn data set *dcbdsn_name* has an invalid dsorg.... 736
550: MKD failed. Dcbdsn data set *dcbdsn_name* has a recfm of *recfm* which is invalid for a PDS.... 737
550: MKD failed. Dcbdsn data set *dcbdsn_name* is migrated and noautorecall is specified.... 737
550: MKD failed. Error locating dcbdsn data set *dcbdsn_name*.... 738
550: MKD failed. Unit=*unit_name* invalid for PDS.... 738
550: MKD failed. Volume for dcbdsn data set *dcbdsn_name* is not mounted and NoAutomount is specified.... 738
550: MKD failed. Volume list *volume serial list* includes a volume which is not mounted and NoAutoMount is specified.... 739
550: MKD failed. Volume *volume* is not mounted and NoAutoMount is specified.... 739
550: MKD failed. Volume=*serial* is a tape and is invalid for a PDS.... 740
550: MKD failed. Volume=*volume serial list* includes a tape and is not valid for a PDS.... 740
550: MKD failed. Error mounting dcbdsn data set *dcbdsn_name*.... 741
550: MKD failed. Error retrieving dcbdsn data set *dcbdsn_name*.... 741
550: MKD failed. Recfm *recfm* is invalid for a PDS.... 742
550: Mkd fails: *new_directory*. User not authorized.... 742
550: MKDIR failed: *error*.... 742
550: Name length error for pathname *pathname*.... 743

550: No data sets found....743
550: No jobs found for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner*....744
550: No members found....744
550: No spool files available for *jobid*....744
550: No spool files available for *jobid*, JesPutGet aborted....745
550: Non-DASD data set *dsname* cannot be processed....745
550: Open of *dsname* failed....745
550: Partitioned data set '*pathname*' does not exist....746
550: Pathname does not contain valid Jobid....746
550: pathname *pathname* not retrievable....747
550: Permanent negative completion....747
550: READTAPEFormat value is *value* but input tape is *format*....747
550: READTAPEFormat *value* is value but input tape is format *format*....748
550: READTAPEFormat value is *value* but input tape is not spanned....748
550: READTAPEFormat value is *value* but input tape is spanned....749
550: Rename fails: *dsname* already exists....749
550: Rename fails: GDG name conversion failed....750
550: Renaming attempt failed. Rc was *errno*....750
550: Request nonexistent member *file_name* to be sent....750
550: request size of nonexistent member *member*....751
550-: Request to export security context failed....751
550: Retrieval of a whole partitioned data set is not supported. Use MGET or MVSGET for this purpose....751
550: RMD failed. Valid only for z/OS UNIX files or partitioned data sets....752
550: Rmd fails: *directory*. User not authorized....752
550: RMDIR failed: *error*....752
550: RNFR fails: *dsname* does not exist....753
550: RNFR fails: *dsname*. User not authorized....753
550: RNTO fails: *dsname*. User not authorized....753
550 : SIZE command not supported with active security mechanism....754
550: Size of a whole Partitioned data set is not supported....754
550: SIZE fails: *file name* is migrated....754
550: SIZE fails: *filename* is on a volume which is not mounted....755
550: SQL query not available. Can't load CAF routines....755
550-: SVC99 RETURN CODE=*rc* S99INFO=*info* S99ERROR=*decerr* HEX=*hexerr* S99ERSN code *code*. 756
550-: System completion code and reason: *code-reason*....756
550: TAPEREADSTREAM does not support transfer of an American Standards Association (ASA) data set....757
550: TAPEREADSTREAM does not support transfer of the trailing blanks in a fixed format tape data set....757
550: The user is not authorized to access the job....758
550: Transfer aborted....758
550: TYPE U transfer requires variable format data set....758
550: Unable to append to *dsname*....759
550: Unable to append to fixed record format file in image mode....759
550: Unable to append to member *name* in Partitioned data set *dsname*....759
550: Unable to append to the Null directory....760
550: Unable to create data set *dsname* for *command* command....760
550: Unable to delete *directory* (Error code: *error_code*, Reason code: *reason_code*, S99ERSN code *s99reason_code*)....760
550: Unable to delete *dsname* (Rc = *errno*)....761
550: Unable to obtain data set list....761
550-: Unable to obtain JES NODE name from subsystem information....762
550: Unable to perform LIST/NLST command due to error with /dev/null....762
550: Unable to send *dsname*....762
550: Unable to size *dsname*....763
550: Unable to store *dsname*....763

550: Unable to store member *name* in Partitioned data set *dsname*.... 763
550: Unable to store unique *dsname*.... 764
550: Unable to store unique member *name* in Partitioned data set *dsname*.... 764
550: Unexpected status for *dsname*.... 764
550: Unknown HOME directory for pathname *path*....765
550: Unknown return code from Get JES spool request: *number*....765
550: Unknown return code from Get JES spool request: *number*, JesPutGet aborted....765
550: Unknown return code from JES cancel request.... 766
550: User Exit refuses this Job to be submitted by *dsname*.... 766
550: Volume containing *dsname* is not mounted and NoAutoMount specified....766
550-: volume for "*new_directory*" is not mounted and NoAutomount is specified.... 767
550: Volume is not ready and automatic tape mounts are not allowed....767
550: Volume *name* is not mounted and NoAutoMount is specified.... 767
550: Volume=*volume list* includes a volume which is is not mounted and NoAutoMount is specified.... 768
550: VSAM data set *dsname* cannot be processed....768
551 reply codes.... 768
551: command terminated due to server shutdown in progress.... 769
551: Reload of the load library failed.... 769
551: Transfer aborted: attempt to connect to *db2name* failed *(code)*....769
551: Transfer aborted: *condition* occurred for TYPE U transfer.... 770
551: Transfer aborted: conversion failure....770
551: Transfer aborted: internal read error.... 770
551: Transfer aborted: internal write error....771
551: Transfer aborted: SQL CURSOR DECLARE failure....771
551: Transfer aborted: SQL CURSOR OPEN failure....771
551: Transfer aborted: SQL not available. Attempt to open plan *plan_name* failed *(code)*.... 772
551: Transfer aborted: SQL PREPARE/DESCRIBE failure....772
551: Transfer aborted: uneven number of bytes received for TYPE U transfer.... 773
551: Unload of the load library failed....773
552 reply codes.... 773
552: Command *cmd* fails: *filename* does not exist.... 773
554 reply codes.... 774
554: command terminated due to server shutdown in progress.... 774
554: Multibyte transfer not supported for destination processing.... 774
554: Requested action not taken: file not found....775
554: Requested action not taken: GDG name conversion failed....775
554: Requested action not taken: invalid REST parameter.... 776
554: Restart not valid for destination processing.... 776
554: Transfer aborted: unsupported SQL statement....776
557 reply codes.... 777
557 : Data contains codepoints that cannot be translated.... 777
557 : File contains ASCII data - enter TYPE A command before entering *cmdname* command.... 777
557 : File contains binary data - enter TYPE I command before entering *cmdname* command 778
557 : JES functions are not allowed with ASCII codepage *codepage*....778

Chapter 18. Intrusion detection services probeids.... 779

Chapter 19. Resolver return and reason codes.... 789
Resolver return codes....789
Resolver reason codes....790

Chapter 20. TCP/IP Discard reason codes.... 793

Chapter 21. ENF event code 80 return and reason codes.... 807

Appendix A. Related protocol specifications.... 809

Appendix B. Architectural specifications..... 829

Appendix C. Accessibility.....831

Notices.....833
Terms and conditions for product documentation..... 834
IBM Online Privacy Statement..... 835
Policy for unsupported hardware.....835
Minimum supported hardware.....835
Policy for unsupported hardware.....836
Trademarks..... 836

Bibliography.....837

Index..... 841

Communicating your comments to IBM..... 843

Figures

1. Sense data format..... 1

2. Contents of the diagnostic code for cause codes 1, 2, and 49.....324

3. Contents of the diagnostic code for cause codes 21..... 325

4. Contents of the VPCI/VCI diagnostic code.....328

5. Contents of the message type diagnostic code..... 328

6. Contents of the timer number diagnostic code.....330

Tables

1. Usage of hexadecimal 1008 sense code specific information by LU type..... 104

2. Sense field values..... 144

3. SNA sense information received at the application program..... 145

4. Explanation of USENSEI Information..... 145

5. MAC generic codes..... 207

6. MAC LAN specific codes..... 208

7. LLC LAN generic codes..... 211

8. LLC LAN specific codes..... 212

9. Byte 0 (category) of the DLC status code..... 223

10. Byte 1 (reporting layer identifier and location) of the DLC status code..... 224

11. Bytes 2 and 3 (completion code) of the DLC status code..... 225

12. Resource state code values..... 266

13. Resource status modifiers..... 283

14. Resource status field information..... 283

15. Session initiation states..... 285

16. ATM network-generated cause codes..... 317

17. ATM network-generated coding standard..... 323

18. ATM network-generated cause location..... 324

19. Diagnostic code for cause codes 1, 2, and 49..... 325

20. Diagnostic code for cause code 21..... 326

21. Virtual path connection identifier and virtual channel identifier..... 328

22. Message type..... 329

23. Timer number..... 331

24. Sockets ERRNOs..... 355

25. Sockets extended ERRNOs.....366

26. Intrusion detection services probeids..... 780

27. Resolver return codes for getaddrinfo, getnameinfo, and freeaddrinfo.....789

28. Resolver return codes for gethostbyname and gethostbyaddr..... 790

29. Resolver reason codes.....790

30. Packet trace discard reason codes for the IP protocol.....793

31. Packet Trace Discard reason codes for the TCP Protocol.....800

32. Packet Trace Discard reason codes for the UDP Protocol..... 803

33. Packet Trace Discard reason codes for the RAW Protocol..... 805

34. Return codes and reason codes for ENF event code 80 processing..... 807

About this document

This document describes VTAM® or TCP/IP codes. Use this document to look up specific VTAM or TCP/IP codes. For background reading to help understand concepts involved in VTAM operations, and for examples of the message output for a variety of DISPLAY commands, see the z/OS Communications Server: SNA Operation.

The information in this document supports both IPv6 and IPv4. Unless explicitly noted, information describes IPv4 networking protocol. IPv6 support is qualified within the text.

This document refers to Communications Server data sets by their default SMP/E distribution library name. Your installation might, however, have different names for these data sets where allowed by SMP/E, your installation personnel, or administration staff. For instance, this document refers to samples in SEZAINST library as simply in SEZAINST. Your installation might choose a data set name of SYS1.SEZAINST, CS390.SEZAINST, or other high level qualifiers for the data set name.

Who should read this document

This document is written for anyone required to interpret a VTAM or TCP/IP code. Familiarity with VTAM and TCP/IP concepts and terms is assumed.

How this document is organized

This document contains the following information:

- Chapter 1, “SNA sense codes,” on page 1, contains all sense codes set by VTAM and sense fields for RPL-based macros. Because sense codes can be set by many different products, this does not include all sense codes that can display in VTAM messages.
- Chapter 2, “Return codes for VTAM macroinstructions,” on page 147, describes return codes that are displayed in VTAM messages.
- Chapter 3, “Data link control (DLC) status codes,” on page 223, contains the data link control (DLC) status codes issued in some messages and in the IUTx VIT entry.
- Chapter 4, “CSM monitor IDs,” on page 261, contains the CSM Monitor IDs.
- Chapter 5, “VTAM status codes,” on page 265, includes resource status and session state codes and modifiers.
- Chapter 6, “VTAM wait state event codes and IDs,” on page 293, includes the wait state event codes that are displayed in VTAM messages.
- Chapter 7, “VTAM abend codes,” on page 307, describes VTAM abend codes.
- Chapter 8, “ATM network-generated cause and diagnostic codes,” on page 317, contains the ATM network-generated cause and diagnostic codes issued in some messages.
- Chapter 9, “SNA coupling facility user reason codes,” on page 333, describes the user reason codes issued to MVS™ by the Coupling Facility.
- Chapter 10, “TCP/IP codes,” on page 335, contains the FTP Server, MVP, SMTP, and SNA LU 6.2 codes.
- Chapter 11, “SNMP pe_error messages,” on page 349, contains descriptions of the pe_errors that can appear when SNMPD is decoding the presentation elements from a presentation stream.
- Chapter 12, “SNMP ps_error messages,” on page 351, contains descriptions of the ps_errors that can appear when SNMPD is converting a presentation stream into a series of presentation elements.
- Chapter 13, “Sockets and sockets extended return codes (ERRNOs),” on page 355, contains a table showing the system-wide message numbers and codes set by the system calls.
- Chapter 14, “TCP/IP abend 3C5 reason codes,” on page 371, contains a table showing the reason codes for abend 3C5.

© Copyright IBM Corp. 2000, 2021

- Chapter 15, “TCP/IP abend 422 reason codes,” on page 399, contains a description of the abend 422 reason codes.
- Chapter 16, “TCP/IP abend 4C5 reason codes,” on page 401, contains a table showing the reason codes for abend 4C5.
- Chapter 17, “FTPD reply codes,” on page 425, contains a description of the FTPD Reply codes.
- Chapter 18, “Intrusion detection services probeids,” on page 779, contains a description of the Intrusion Detection Services probeids to identify the reason and code location associated with output information.
- Chapter 19, “Resolver return and reason codes,” on page 789, contains a description of the return codes and the reason codes generated by the Resolver.
- Chapter 20, “TCP/IP Discard reason codes,” on page 793, contains a description of the discard reason codes used by the IP layer and the TCP protocol layer.
- Appendix A, “Related protocol specifications,” on page 809, lists the related protocol specifications for TCP/IP.
- Appendix C, “Accessibility,” on page 831, describes accessibility features to help users with physical disabilities.
- “Notices” on page 833, contains notices and trademarks used in this document.
- “Bibliography” on page 837, contains descriptions of the documents in the z/OS® Communications Server library.

How to use this document

To use this document, you should be familiar with the z/OS TCP/IP services and the TCP/IP suite of protocols.

How to contact IBM service

For immediate assistance, visit this website: https://www.ibm.com/mysupport

Most problems can be resolved at this website, where you can submit questions and problem reports electronically, and access a variety of diagnosis information.

For telephone assistance in problem diagnosis and resolution (in the United States or Puerto Rico), call the IBM Software Support Center anytime (1-800-IBM®-SERV). You will receive a return call within 8 business hours (Monday – Friday, 8:00 a.m. – 5:00 p.m., local customer time).

Outside the United States or Puerto Rico, contact your local IBM representative or your authorized IBM supplier.

If you would like to provide feedback on this publication, see “Communicating your comments to IBM” on page 843.

Conventions and terminology that are used in this information

Commands in this information that can be used in both TSO and z/OS UNIX environments use the following conventions:

- When describing how to use the command in a TSO environment, the command is presented in uppercase (for example, NETSTAT).
- When describing how to use the command in a z/OS UNIX environment, the command is presented in bold lowercase (for example, **netstat**).
- When referring to the command in a general way in text, the command is presented with an initial capital letter (for example, Netstat).

All the exit routines described in this information are *installation-wide exit routines*. The installation-wide exit routines also called installation-wide exits, exit routines, and exits throughout this information.

The TPF logon manager, although included with VTAM, is an application program; therefore, the logon manager is documented separately from VTAM.

Samples used in this information might not be updated for each release. Evaluate a sample carefully before applying it to your system.

z/OS no longer supports mounting HFS data sets (The POSIX style file system). Instead, a z/OS File System (ZFS) can be implemented. The term hierarchical file system, abbreviated as HFS, is defined as a data structure that has a hierarchical nature with directories and files. References to hierarchical file systems or HFS might still be in use in z/OS Communications Server publications.

Note: In this information, you might see the following Shared Memory Communications over Remote Direct Memory Access (SMC-R) terminology:

- RoCE Express®, which is a generic term representing IBM 10 GbE RoCE Express, IBM 10 GbE RoCE Express2, and IBM 25 GbE RoCE Express2 feature capabilities. When this term is used in this information, the processing being described applies to all of these features. If processing is applicable to only one feature, the full terminology, for instance, IBM 10 GbE RoCE Express will be used.
- RoCE Express2, which is a generic term representing an IBM RoCE Express2® feature that might operate in either 10 GbE or 25 GbE link speed. When this term is used in this information, the processing being described applies to either link speed. If processing is applicable to only one link speed, the full terminology, for instance, IBM 25 GbE RoCE Express2 will be used.
- RDMA network interface card (RNIC), which is used to refer to the IBM 10 GbE RoCE Express, IBM® 10 GbE RoCE Express2, or IBM 25 GbE RoCE Express2 feature.
- Shared RoCE environment, which means that the "RoCE Express" feature can be used concurrently, or shared, by multiple operating system instances. The feature is considered to operate in a shared RoCE environment even if you use it with a single operating system instance.

Clarification of notes

Information traditionally qualified as Notes is further qualified as follows:

Attention
Indicate the possibility of damage

Guideline
Customary way to perform a procedure

Note
Supplemental detail

Rule
Something you must do; limitations on your actions

Restriction
Indicates certain conditions are not supported; limitations on a product or facility

Requirement
Dependencies, prerequisites

Result
Indicates the outcome

Tip
Offers shortcuts or alternative ways of performing an action; a hint

Prerequisite and related information

z/OS Communications Server function is described in the z/OS Communications Server library. Descriptions of those documents are listed in “Bibliography” on page 837, in the back of this document.

Required information

Before using this product, you should be familiar with TCP/IP, VTAM, MVS, and UNIX System Services.

Softcopy information

Softcopy publications are available in the following collection.

Titles	Description
IBM Z Redbooks	The IBM Z®® subject areas range from e-business application development and enablement to hardware, networking, Linux®, solutions, security, parallel sysplex, and many others. For more information about the Redbooks® publications, see http://www.redbooks.ibm.com/ and http://www.ibm.com/systems/z/os/zos/zfavorites/.

Other documents

This information explains how z/OS references information in other documents.

When possible, this information uses cross-document links that go directly to the topic in reference using shortened versions of the document title. For complete titles and order numbers of the documents for all products that are part of z/OS, see z/OS Information Roadmap (SA23-2299). The Roadmap describes what level of documents are supplied with each release of z/OS Communications Server, and also describes each z/OS publication.

To find the complete z/OS library, visit the z/OS library in IBM Documentation (https://www.ibm.com/docs/en/zos).

Relevant RFCs are listed in an appendix of the IP documents. Architectural specifications for the SNA protocol are listed in an appendix of the SNA documents.

The following table lists documents that might be helpful to readers.

Title	Number
DNS and BIND, Fifth Edition, O'Reilly Media, 2006	ISBN 13: 978-0596100575
Routing in the Internet, Second Edition, Christian Huitema (Prentice Hall 1999)	ISBN 13: 978-0130226471
sendmail, Fourth Edition, Bryan Costales, Claus Assmann, George Jansen, and Gregory Shapiro, O'Reilly Media, 2007	ISBN 13: 978-0596510299
SNA Formats	GA27-3136
TCP/IP Illustrated, Volume 1: The Protocols, W. Richard Stevens, Addison-Wesley Professional, 1994	ISBN 13: 978-0201633467
TCP/IP Illustrated, Volume 2: The Implementation, Gary R. Wright and W. Richard Stevens, Addison-Wesley Professional, 1995	ISBN 13: 978-0201633542
TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols, W. Richard Stevens, Addison-Wesley Professional, 1996	ISBN 13: 978-0201634952
TCP/IP Tutorial and Technical Overview	GG24-3376
Understanding LDAP	SG24-4986
z/OS Cryptographic Services System SSL Programming	*SC14-7495*
z/OS IBM Tivoli Directory Server Administration and Use for z/OS	*SC23-6788*
z/OS JES2 Initialization and Tuning Guide	*SA32-0991*
z/OS Problem Management	*SC23-6844*
z/OS MVS Diagnosis: Reference	*GA32-0904*
z/OS MVS Diagnosis: Tools and Service Aids	*GA32-0905*
z/OS MVS Using the Subsystem Interface	*SA38-0679*

Title	Number
z/OS Program Directory	*GI11-9848*
z/OS UNIX System Services Command Reference	*SA23-2280*
z/OS UNIX System Services Planning	*GA32-0884*
z/OS UNIX System Services Programming: Assembler Callable Services Reference	*SA23-2281*
z/OS UNIX System Services User's Guide	*SA23-2279*
z/OS XL C/C++ Runtime Library Reference	*SC14-7314*
Open Systems Adapter-Express Customer's Guide and Reference	*SA22-7935*

Redbooks publications

The following Redbooks publications might help you as you implement z/OS Communications Server.

Title	Number
IBM z/OS Communications Server TCP/IP Implementation, Volume 1: Base Functions, Connectivity, and Routing	SG24-8096
IBM z/OS Communications Server TCP/IP Implementation, Volume 2: Standard Applications	SG24-8097
IBM z/OS Communications Server TCP/IP Implementation, Volume 3: High Availability, Scalability, and Performance	SG24-8098
IBM z/OS Communications Server TCP/IP Implementation, Volume 4: Security and Policy-Based Networking	SG24-8099
IBM Communication Controller Migration Guide	SG24-6298
IP Network Design Guide	SG24-2580
Managing OS/390 TCP/IP with SNMP	SG24-5866
Migrating Subarea Networks to an IP Infrastructure Using Enterprise Extender	SG24-5957
SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements	SG24-5631
SNA and TCP/IP Integration	SG24-5291
TCP/IP in a Sysplex	SG24-5235
TCP/IP Tutorial and Technical Overview	GG24-3376
Threadsafe Considerations for CICS	SG24-6351

Where to find related information on the Internet

z/OS

This site provides information about z/OS Communications Server release availability, migration information, downloads, and links to information about z/OS technology

http://www.ibm.com/systems/z/os/zos/

z/OS Internet Library

Use this site to view and download z/OS Communications Server documentation

http://www.ibm.com/systems/z/os/zos/library/bkserv/

z/OS Communications Server product

The page contains z/OS Communications Server product introduction

https://www.ibm.com/products/zos-communications-server

IBM Communications Server product support

Use this site to submit and track problems and search the z/OS Communications Server knowledge base for Technotes, FAQs, white papers, and other z/OS Communications Server information

https://www.ibm.com/mysupport

IBM Communications Server performance information

This site contains links to the most recent Communications Server performance reports

http://www.ibm.com/support/docview.wss?uid=swg27005524

IBM Systems Center publications

Use this site to view and order Redbooks publications, Redpapers, and Technotes

http://www.redbooks.ibm.com/

z/OS Support Community

Search the z/OS Support Community Library for Techdocs (including Flashes, presentations, Technotes, FAQs, white papers, Customer Support Plans, and Skills Transfer information)

z/OS Support Community

Tivoli® NetView® for z/OS

Use this site to view and download product documentation about Tivoli NetView for z/OS

http://www.ibm.com/support/knowledgecenter/SSZJDU/welcome

RFCs

Search for and view Request for Comments documents in this section of the Internet Engineering Task Force website, with links to the RFC repository and the IETF Working Groups web page

http://www.ietf.org/rfc.html

Internet drafts

View Internet-Drafts, which are working documents of the Internet Engineering Task Force (IETF) and other groups, in this section of the Internet Engineering Task Force website

http://www.ietf.org/ID.html

Information about web addresses can also be found in information APAR II11334.

Note: Any pointers in this publication to websites are provided for convenience only and do not serve as an endorsement of these websites.

DNS websites

For more information about DNS, see the following USENET news groups and mailing addresses:

USENET news groups
comp.protocols.dns.bind

BIND mailing lists
https://lists.isc.org/mailman/listinfo

BIND Users

- Subscribe by sending mail to bind-users-request@isc.org.
- Submit questions or answers to this forum by sending mail to bind-users@isc.org.

BIND 9 Users (This list might not be maintained indefinitely.)

- Subscribe by sending mail to bind9-users-request@isc.org.
- Submit questions or answers to this forum by sending mail to bind9-users@isc.org.

The z/OS Basic Skills Information Center

The z/OS Basic Skills Information Center is a web-based information resource intended to help users learn the basic concepts of z/OS, the operating system that runs most of the IBM mainframe computers in use today. The Information Center is designed to introduce a new generation of Information Technology professionals to basic concepts and help them prepare for a career as a z/OS professional, such as a z/OS systems programmer.

Specifically, the z/OS Basic Skills Information Center is intended to achieve the following objectives:

- Provide basic education and information about z/OS without charge
- Shorten the time it takes for people to become productive on the mainframe
- Make it easier for new people to learn z/OS

To access the z/OS Basic Skills Information Center, open your web browser to the following website, which is available to all users (no login required): https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zbasics/homepage.html?cp=zosbasics

Summary of changes for IP and SNA Codes

This document contains terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Changes made in z/OS Communications Server Version 2 Release 5

This document contains information previously presented in z/OS Communications Server: IP and SNA Codes, which supported z/OS Version 2 Release 4.

Changed information

- Removal of CMIP from VTAM, see the following topics:
  - "Sense code 086F" on page 64
  - "Sense code 08A9" on page 96
- Shared Memory Communications multiple IP subnet support (SMCv2), see the following topic:
  - Chapter 3, "Data link control (DLC) status codes," on page 223

Changes made in z/OS Communications Server Version 2 Release 4

This document contains information previously presented in z/OS Communications Server: IP and SNA Codes, which supported z/OS Version 2 Release 3.

Changed information

- Network support for z/OS Container Extensions, see Chapter 3, "Data link control (DLC) status codes," on page 223.

Changes made in z/OS Communications Server Version 2 Release 3

This document contains information previously presented in z/OS Communications Server: IP and SNA Codes, which supported z/OS Version 2 Release 2.

December 2018

Changed information

Technical and terminology changes about Shared Memory Communications

March 2018

Changed information

HiperSockets Converged Interface support, see Chapter 3, "Data link control (DLC) status codes," on page 223.

September 2017

Changed information

- 3270 Intrusion Detection Services, see the following topics:
  - "Sense code 082B" on page 40

© Copyright IBM Corp. 2000, 2021

  - “Session status modifiers (positions 6–8)” on page 291
- Communications Server support for RoCE Express2 feature, see Chapter 3, “Data link control (DLC) status codes,” on page 223.

Deleted information

- Removal of SMTPD & sendmail, all references to SMTP and sendmail are deleted.

Chapter 1. SNA sense codes

This section contains the following sections:

- "08XX (request reject)" on page 2
- "10XX (request error)" on page 98
- "20XX (state error)" on page 120
- "40XX (RH usage error)" on page 123
- "80XX (path error)" on page 124
- "A0XX (RTP sense data)" on page 135
- "FFXX (HPR sense data)" on page 141
- "SNA sense field values for RPL-based macroinstructions" on page 143
- "3270 SNA and non-SNA device sense fields" on page 144

Notes:

- This section contains all sense codes set by VTAM. To assist you in problem determination, a number of SNA-architected sense codes set by products other than VTAM are also included. However, this section does not include all product-specific sense codes that might display in VTAM messages. See *SNA Formats* or *SNA Network Product Formats* for a description of all SNA-architected sense codes.
- If a sense code is set by NCP, NetView, CICS®, a device, or any other product, see the appropriate product documentation for a complete explanation of the sense code.
- The SNA sense code definitions used in this section are the architected descriptions written at the time this document was published. Additional VTAM information or helpful hints might be added to the basic SNA definition.

Sense codes

Sense data in a request/response unit (RU) consists of one byte for the category, one byte for the modifier, and two bytes for either sense-code-specific information or user-defined data. Following is the format of sense data:

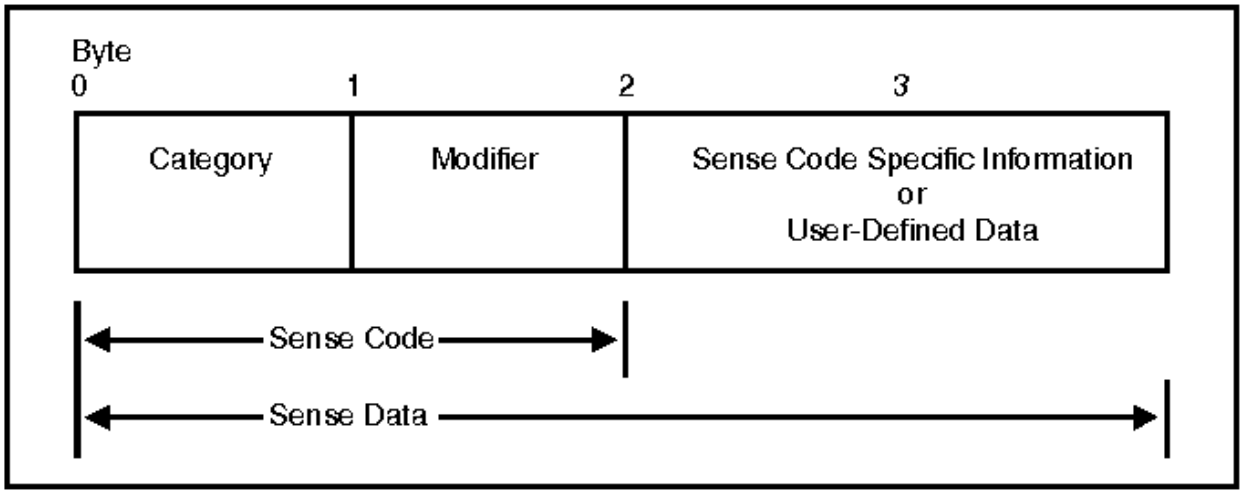

Figure 1. Sense data format

© Copyright IBM Corp. 2000, 2021

08XX (request reject)

This category indicates that the request was delivered to the intended component; it was understood and supported, but not executed.

Sense code 0801

Resource not available: The LU, PU, link station, or link specified in an RU is not available.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- A CINIT request fails because an application rejects a terminal log on. Message IST663I is displayed when this error occurs, and the logon from the terminal fails with USSMSG07. See the information about common subarea network problems in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this problem.
- The logmode is incorrect.
- The major node is not active for the resource. (A frequent reason for this error is that the NCP has not been activated.)
- The line is inactive.
- The line is a CALL=INOUT line over which simultaneous connections are being attempted (dial-in and dial-out). This is a temporary condition and the session might be tried again.
- APPC=YES was coded on the APPL definition, and there is an attempt to establish the session using OPNDST.
- With NTRI, this error can occur when DIALNO is incorrect.
- For IMS, the LU might not be defined.

0001
Independent LU does not receive ACTLU: An ACTLU has been sent by the SSCP to an independent LU (sent by BF).

0002
Reserved resources requested for sessions exceed allowable maximum: The resource reservation request in RNAA exceeds the maximum allowed by system definition. The address was not assigned and no change was made to the current reservation of resources for the LU.

0003
Name aliasing cannot be performed because the name alias function is not available.

0004
A switched connection currently exists for the link being activated, and the SSCP or the subarea PU does not support the protocols necessary to allow takeover of such a link.

0005
A SETCV has been received for a resource that is still represented in the pool of available control blocks.

0006
The line is not associated with a line adapter, or the line is associated with a line adapter that is not valid for the genned usage tier.

0007
The line is associated with a line adapter that is not installed or not attached to the CCU.

0008
The line is associated with a line adapter that is inoperative.

0009
The LU is not available because it is not ready to accept sessions.

000A
The PLU is not available because it is being taken down or has issued SETLOGON with the OPTCD=QUIESCE. The PLU is, therefore, not accepting new sessions. The initiation request should not be tried again.

VTAM hint: If the PLU is TSO, then it is likely that the TSO USERMAX limit has been reached. If a MODIFY TSO,USERMAX=0 was issued, then all LOGON attempts for TSO will fail with this sense code.

000B
The PLU is not available because it is unable to comply with the PLU-SLU role specification.

000C
The SLU is not available because it is unable to comply with the PLU-SLU role specification.

000D
The LU is not available because its SSCP is in the process of being taken down, and is therefore not allowing new sessions to be started. The initiation request should not be tried again.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: A possible cause of this error is that a dynamic application program is trying to open its ACB at the same time its SSCP is in the process of being taken down.

000E
The LU is not available because an intermediate gateway SSCP is in the process of being taken down, and is therefore not allowing new sessions to be started.

000F
The SLU is not available because it is being taken down, and is therefore not accepting new sessions. The initiation request should not be tried again.

0010
A switched subarea connection cannot be established because no switched subarea links are defined.

0011
Switched subarea connection to another network cannot be established because no switched subarea links are defined within a gateway NCP.

0012
An APPN connection cannot be established because this node has no available integers to represent a new TG.

0013
Switched connection cannot be established because a SHM GROUP was not defined in the switched PU's PATH definitions.

0014
A switched connection cannot be established. Call request verification was requested, but is not supported for this configuration. This condition results from conflicting system definition.

0015
The link connection is unavailable as a result of a hardware failure within the line adapter.

0016
A link resource is not available as a result of maintenance occurring on the supporting hardware.

0017
A link resource is not available because a mismatch exists within the microcode of the supporting hardware.

0018
Activation of the channel link failed because the supporting hardware is undergoing error recovery.

0019
Activation of the channel link failed because the supporting hardware is undergoing concurrent maintenance.

001A
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

001B
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

001C
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

001D
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

001E
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

001F
A link connection is associated with a protocol that is inoperative.

0020
A link resource is not available because of a mismatch between current operational parameters and the values specified at system generation.

0026
The PU is not available because the dependent LU server-dependent LU requester connection could not be established.

0027
A switched connection cannot be established because no switched link has been defined.

VTAM hint: A switched connection cannot be established because a GROUP was not defined in the switched PU's PATH definitions or the defined GROUP does not exist in any active NCP major node.

0028
REQDACTPU was received for a PU that is known but whose SSCP-PU session is currently inactive.

0029
A multipath channel connection cannot be established because the system level is not at least MVS 4.3.

002A
An ACTLINK has been received for a resource that is still represented in the pool of available control blocks.

002B
Resource is unavailable due to program or operator action. This sense code is returned by the DLU network node server when it performs resource verification reduction for a DLU in its domain which has registered itself as unavailable for an unexpired time.

002C
The required extended coupling facility is not available.

002E
Generic Resource exit indicated to fail this session.

4001
Line cannot be force deactivated while panel line test is active.

4002
A forced deactivate was attempted when wrap test was active.

Sense code 0802

Intervention required: Forms or cards are required at an output device, or a device is temporarily in local mode, or other conditions require intervention.

Sense code 0803

Missing password: The required password was not supplied.

Sense code 0804

Password was not valid.

Sense code 0805

Session limit exceeded: The requested session cannot be activated, as one of the NAUs is at its session limit, for example, the LU-LU session limit or the (LU, mode) session limit. This sense code applies to ACTCDRM, INIT, BIND, and CINIT requests.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: Possible causes of this error include:

- A dynamic reconfiguration (DR) mismatch exists between VTAM and NCP. Check the PUDR and LUDR pools.
- The session limit was exceeded because:
  - The given mode name was found and the limit is currently set to zero, preventing activation of additional sessions.
  - The given mode name cannot be found. The session limit is assumed to be zero.

0001
If accepted, the BIND request would prevent either the receiving LU or the sending LU from activating the number of contention-winner sessions to the partner LU that were agreed upon during a change-number-of-sessions procedure.

0002
If accepted, the BIND request would cause the XRF-backup session limit to be exceeded.

0003
If accepted, the BIND request would cause the XRF-active session limit to be exceeded.

Note: The session limit for XRF-active sessions is one. An XRF-active BIND is valid only if there are no XRF-active or XRF-backup sessions with the receiving SLU.

0004
For an independent LU, the BIND request, if accepted, would cause the system-defined maximum number of sessions (MAXSESS) allowed for any LU to be exceeded for this LU.

0005
The intermediate session router is unable to create a session connector control block. The pool of session connectors is saturated with active sessions and with pending active sessions for which the queue bit was set in the BIND; the BIND should not be tried again.

0006
The intermediate session router is unable to create a session connector control block. The pool of session connectors is saturated with active sessions and with pending active sessions for which the queue bit was not set in the BIND; the BIND should be tried again.

0008
For a dependent LU, if accepted, the BIND request would cause the session limit to be exceeded.

0009
If accepted, the request would cause the PLU session limit to be exceeded.

000A
If accepted, the request would cause the SLU session limit to be exceeded.

000B
The request was rejected because a session already exists between the same LU pair, and at least one of the LUs does not support parallel sessions.

000C
Duplicate controller session attempted.

Sense code 0806

Resource unknown: For example, the request contained a name or address not identifying a PU, LU, SSCP, link, or link station known to the receiver or the sender.

Note: In an interconnected network environment, this sense code might be set by an SSCP in whose subnetwork and domain the LU was expected to reside; it is not set by an SSCP that is only an intermediary on the session-setup path. A gateway SSCP examines the resource identifier control vector in a session setup request (for example, CDINIT), to determine whether the LU is in the SSCP's subnetwork and domain.

Bytes 2 and 3 following the sense code contain sense code-specific information.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: A possible cause of this error is that *uservarname* has been specified on the ID operand of the DISPLAY NCPSTOR command.

0001
The resources identified in an SNA address list (X'04') MS common subvector are unknown to the PU receiving the request.

Note: When this sense data flows in a negative response to a network management vector transport (NMVT), the referenced X'04' subvector is the one that was present in the request NMVT to which the negative response corresponds. When this sense data flows in a sense data (X'7D') MS common subvector, the referenced X'04' subvector is present with the X'7D' subvector in the same major vector.

0002
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM issues this code in response to an NPM session collection request for an undefined resource to indicate that the request was successful.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

0004
The indicated resources in the accompanying name list (X'06') subvector are unknown to the control point to which the request containing the subvector was routed.

Note: Names in the hierarchy below the level of the first unknown resource are not examined by the control point.

0005
The physical unit is currently in the physical unit dynamic reconfiguration pool.

0006
For a dynamic reconfiguration DELETE, MOVE, or REPLACE operation, the resource to be dynamically reconfigured could not be found.

0007
The LU address in bytes 8–9 of RNAA Type X'04' is already in the free pool.

0008
For a dynamic reconfiguration DELETE, MOVE, or REPLACE operation, the NAU name in RNAA does not correspond to the resource identified by the element address in the RNAA.

0009
The SSCP(OLU) cannot identify the SSCP(DLU), and the default SSCP rerouting is not enabled.

000A
The configuration identifier specified in a management services command is not recognized by the DLC manager at the receiving node.

0011
An unknown OLU name was specified in the request.

0012
An unknown DLU name was specified in the request.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- No CDRMs are active.
- No CDRSC exists for the DLU, and one cannot be created dynamically because CDRDYN=NO. Verify that a host CDRM definition exists and is activated if this node was started with a subarea number, and ensure that CDRDYN=YES is specified on the CDRM definition. See z/OS Communications Server: SNA Resource Definition Reference for information about the CDRDYN operand.

0013
An unknown SLU name was specified in the request.

0014
An unknown PLU name was specified in the request.

0015
An unknown OLU address was specified in the request.

0016
An unknown DLU address was specified in the request.

0017
An unknown SLU address was specified in the request.

0018
An unknown PLU address was specified in the request.

0021
The session-initiation request specified that the receiving SSCP is the SSCP having the DLU in its domain, but the DLU is unknown to the receiving SSCP. This error can occur if a CDRM is coded incorrectly on the CDRSC definition statement.

0022
The originator of the request or response is unknown to the receiver.

0023
The destination of the request or response is unknown to the sender.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0024
An unknown LU1 name was specified in the request.

0025
An unknown LU2 name was specified in the request.

0026
The SSCP does not have a session with the boundary function PU of an independent LU.

0027
The PU associated with a switched SLU is unknown. Session setup processing for the switched SLU cannot proceed.

0028
NAU1 network address is unknown.

0029
NAU2 network address is unknown.

002A
The NAU name in the CONTACT or ACTLU does not correspond to the resource at the target address.

002B
The TG being activated is unknown.

002C
The identification supplied by the adjacent node in its XID3 differed from the identification that the receiving node was configured to expect.

002D
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

002E
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

002F
The destination resource was not found on this node during a session activation attempt.

0030
The adjacent node was not identified during CP-CP session activation or deactivation.

0031
Upon receiving a route request from another component in the node, TRS has been unable to locate in its topology database the destination network node or any network node specified in the TG vectors for the destination end node; the request is rejected.

0032
A SETCV defining an intra-FRSE PCV segment subport set was received containing an element address unknown to the receiver.

0033
A network resource needed for session establishment has become unavailable resulting in the termination of the pending session establishment procedure.

0034
REQDACTPU received for an unknown PU.

VTAM hint: This sense code is set by VTAM when processing the REQDACTPU request received from the dependent LU requester (DLUR) to deactivate the PU, but the PU is not known to VTAM. VTAM will send a negative REQDACTPU response with the sense code to the DLUR.

Verify that the PU name is specified correctly in the PU definition for the switched major node and in the DLUR definitions. If you have a system where PUs are being dynamically created, verify that the PU name is specified correctly in either the NIDDEF or CPNDEF definitions and in the DLUR definitions.

0035
The local node has received an unknown adjacent CP name in a request to activate or deactivate a CP-CP session.

0036
No SSCP-SSCP session exists between the VRTG end points.

VTAM Information: VTAM sets this sense code when a CDINIT(5) or DSRLSR(4) cannot be sent because there is no SSCP session between the VR-based TG (VRTG) endpoints. A VRTG, although it creates the appearance of APPN, always represents underlying subarea connectivity and the existing subarea requirement that every SSCP in the network must have an active CDRM session with every other SSCP in that network is still in effect. See the information about VRTGs in z/OS Communications Server: SNA Network Implementation Guide .

3426
Product-specific sense code.

VTAM hint: This sense code can be displayed in a VTAM message but is set by another product. It might be issued by CICS. If issued by CICS, bytes 2 and 3 map to a CICS message number. See http://www.ibm.com/software/htp/cics/library/ for additional information about CICS messages and codes.

Sense code 0807

Resource not available—LUSTAT forthcoming: A subsidiary device will be unavailable for an indeterminate period of time. LUSTAT will be sent when the device becomes available.

Tip: If you receive this sense code while you are trying to establish a connection with a dynamic EE PU, the dialing side of the connection receives an INOP notification. The cause of the problem might be that none of the TGNs specified on the EE model PU are available.

Sense code 0808

The contents ID contained on the ACTCDRM request was not valid.

Sense code 0809

Mode inconsistency: The requested function cannot be performed in the present state of the receiver.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- If resources are not activating correctly when a new NCP is activated, either rename the new NCP or use another method to make sure that the old resource resolution table (RRT) is replaced with the new RRT.
- If you are trying to establish a session to a 3274, this error can occur when DATMODE=HALF is not coded on the PU definition statement.
- A VARY INACT,FORCE command on a switched PU is turned into a VARY INACT,REACT.
- If a USERVAR is defined, the USERVAR name is required for session initiation instead of the real name.
- There is not enough storage to enable VTAM to add a dynamic application program to the symbol resolution table (SRT).
- Another resource with the same name as a dynamic application program that requests to open its ACB has already been defined.

0001
The logical unit vector (LUV) table is too small.

0002
Either the SSCP is not the owner, or it was not added by dynamic reconfiguration.

0003
Previous RNAA received for the same address. Check the LOCADDR in the LU definitions.

0004
Local address X'0000' specified for a logical unit added to a cluster controller module (PU Type 2).

0005
Attempted to switch the line mode when the link was already active.

0006
The logical unit was specified at system generation as not available for dynamic reconfiguration.

0007
Attempted to switch the line mode while an activate link command is in progress.

0008
Attempted to switch the line mode while a deactivate link is in progress.

0009
Attempted to switch the line mode while a wrap is in progress on this line.

000A
Either the specified physical unit was not assigned to the specified link, or the specified logical unit was not assigned to the specified physical unit.

000B
The logical unit or the physical unit was in active session.

000D
A logical unit was still assigned to the physical unit.

000E
The resource to be dynamically reconfigured is a system generated resource and is defined as not DR-deletable.

000F
An RNAA received from an SSCP is rejected because it specifies a resource (adjacent link station or LU) that currently has an address assigned as a result of the RNAA of another SSCP; or an ACTLU, FNA, or SETCV received from an SSCP is rejected because it specifies a resource address that is not assigned to an existing resource or is assigned as a result of the RNAA of another SSCP.

0010–0013
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

0010
Attempted to switch the line mode while a line trace or scanner interface trace (SIT) is in process.

0014
ANS mismatch discovered.

0015
The type modifier (3270 indicator) is already set and does not match the type modifier in this command.

0016
The PU type on SETCV does not match the actual PU type.

0017
The error-recovery modifier is already set and does not match the error-recovery modifier in this command.

0018
The pass limit is already set and does not match the pass limit field in this command.

0019
A SETCV was received containing a value for the SDLC BTU send limit that conflicts with the previous value received.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP, SSP, and EP Messages and Codes* for a complete description.

001A
The maximum segment size is already set and does not match the maximum segment size in this command.

001B
The command specifies a pool indicator that is not X'00' or X'01'.

001C
The RNAA request contains a network ID that is not known to the gateway PU.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

001D
An address-pair session key in a network-qualified address pair control vector (X'15') is not known to the gateway PU.

001E
A gateway PU received an RNAA request for a cross-network session and all possible address transforms for the named resource are allocated.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0020
The gateway node receiving an RNAA request cannot support another session between the named resource pair.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0024
A PU received an ACTPU request with the SSCP-PU session capabilities control vector (X'0B') indicating that the sending SSCP does not support ENA, but the PU does not know the SSCP’s maximum subarea address value.

0025
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP, SSP, and EP Messages and Codes* for a complete description.

0026
MAXOUT of zero received.

0027
A request for a function was received by a component, but the function was not enabled or activated.

0028
Cleanup termination of an LU-LU session has been converted to a forced termination by the LU. The SSCP must wait for session-ended signals before deleting its session awareness records of the session.

0029
Second-level application state change has occurred. An application program served by an MS application program has changed the state of a node that might result in the rejection or failure of a current request or of a future request that would have previously been honored.

002A
The route setup procedure identified in a session services request was not in the expected state.

0030
An FNA was received for an LU that has an active SSCP-LU session.

0031
Bind failure: Mismatch of date, time, or NCP load module name. The load module currently processing in the CCU does not match the NPM resource resolution table (RRT) in use by NPM. The NCP generation date, time, and load module name in the NPM RRT must match that in the NCP exactly. Verification is through the user data in the bind image.

0032
A BFSESSINFO was received when the LU was not pending BFSESSINFO; the reported sessions will be terminated, and the associated network addresses will be freed. This sense data is also included in the BFCLEANUP when the sessions are terminated.

0033
A BIND with the same LFSID as an existing pending-reset session has been received by a boundary function from a peripheral PLU.

0034
A termination request has been received for a resource that has been taken over by an SSCP. The termination type is not strong enough to apply to the resources. The termination type needs to be forced or cleanup.

0035
A cross-domain resource, which was expected to be active, is inactive.

0036
The short hold mode logical connection selected does not exist.

0037
A non-short hold mode connection was attempted on a port (group) that is dedicated to short hold mode operation.

0038
There is an inconsistency of mode between the XID sender and receiver. The XID receiver is operating in short hold mode. Examples include inconsistent settings of the short hold indicator (SHI), the short hold status indicator (SHSI), and the XID exchange state indicator.

0039
CP Transaction Error: CP Capabilities (X'12C1') GDS variable request sent indicating conversation complete or without change direction (CEB or ¬CD) or CP Capabilities reply sent indicating conversation not yet complete (¬CEB).

VTAM hint: This sense code is set by VTAM in the following situations:

- During contention winner CP-CP session activation.
  - The execution of an APPCCMD CONTROL=ALLOC,QUALIFY=CONWIN instruction to allocate a conwinner CP-CP session failed due to an unrecoverable error, and APPC did not communicate

to the issuing TP a non-zero sense code at the time the ALLOC instruction was posted back. The RCPRI and RCSEC return codes displayed in message IST1002I in the IST1110I message group provide more information about the cause of the error.

- The execution of the APPCCMD CONTROL=RECEIVE,QUALIFY=SPEC instruction to receive the capabilities of the adjacent CP completed successfully, but the TP issuing that instruction was not notified that the partner LU has unconditionally deallocated the conversation. You might want to make the system programmer aware of this situation.

- During contention loser CP-CP session activation.
  - The execution of the APPCCMD CONTROL=RECEIVE,QUALIFY=SPEC instruction to receive the capabilities of the adjacent CP completed successfully, but the partner LU did not enter RECEIVE state as expected. You might want to make the system programmer aware of this situation.
- During contention winner or contention loser CP-CP session activation.
  - The execution of an APPCCMD CONTROL=SEND,QUALIFY=DATA instruction to send our CP capabilities to the adjacent CP failed due to an unrecoverable error, and APPC did not communicate to the issuing TP a non-zero sense code at the time the SEND was posted back. The RCPRI and RCSEC return codes displayed in message IST1002I in the IST1110I message group provide more information about the cause of the error.
  - The execution of the APPCCMD CONTROL=RECEIVE,QUALIFY=SPEC instruction to receive the adjacent CP's capabilities failed due to an unrecoverable error, and APPC did not communicate to the issuing TP a non-zero sense code at the time the RECEIVE was posted back. The RCPRI and RCSEC return codes displayed in message IST1002I in the IST1110I message group provide more information about the cause of the error.
  - The execution of the APPCCMD CONTROL=RECEIVE,QUALIFY=SPEC instruction to receive the adjacent CP's capabilities completed successfully, but something other than data was received from the partner CP. You might want to make the system programmer aware of this situation.

003A
A null XID was received when an XID3 with its exchange state indicators set to "prenegotiation," "negotiation proceeding,"or "exchange state indicators not supported" was expected.

003B
A null XID was received when a nonactivation XID3 was expected.

003C
An XID3 with the exchange state indicators set to "prenegotiation"was received when either of the values "negotiation proceeding" or "exchange state indicators not supported" was expected.

003D
A nonactivation XID3 was received when a null XID or link-activation XID3 was expected.

003E
A link activation XID3 was received when a null XID or nonactivation XID3 was expected.

003F
The node with a secondary link station attempted to initiate a nonactivation exchange when secondary-initiated nonactivation exchanges are not supported on the connection.

0040
A mode-setting command was received and was either not expected or not valid for the receiving node; for example, SNRME was received when SNRM was expected.

0041
An XID3 with the Exchange State indicators specifying a negotiation-proceeding exchange was received when an XID3 indicating a prenegotiation exchange was expected. If prenegotiation XID3s are used in a link activation XID exchange, each node must send and receive one.

0042
On an ABM TG on which secondary-initiated nonactivation XID exchanges are supported, the adjacent link station has initiated a nonactivation exchange by sending a nonactivation XID3 in which the ABM Nonactivation XID Exchange Initiator indicator specifies that the sending node is not initiating

a nonactivation exchange. On such TGs, the initiator of a nonactivation exchange always explicitly indicates that it is initiating a nonactivation exchange.

0046
An XID3 indicating that the sender supports the Exchange State indicators was received when the sender had previously indicated that it does not support this field in XID3.

0047
An XID has been received after receipt of a mode-setting command but before the completion of the mode-setting sequence, for example, before RR, RNR, or an I-frame with the poll bit set has been sent by the node with the primary link station after it has received UA in response to its mode-setting command.

0048
A node with an NRM primary link station has received an XID3 when it has no outstanding commands. NRM secondary link stations send XIDs only in response to XID commands.

0049
The XID3 received from the adjacent node had an XID negotiation error (X'22') control vector appended. The XID exchange will therefore terminate unsuccessfully.

004A
The request cannot be accepted because dynamic reconfiguration is in process for the target resource.

004B
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP, SSP, and EP Messages and Codes* for a complete description.

004C
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP, SSP, and EP Messages and Codes* for a complete description.

004D
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP, SSP, and EP Messages and Codes* for a complete description.

004E
A node with a secondary NRM link station attempted to initiate a nonactivation XID exchange with an XID3. Nodes with secondary NRM link stations can solicit a nonactivation XID3 exchange only by sending a null XID at a response opportunity.

0050
An UNBIND request was received on behalf of a resource for which a previous UNBIND is in progress. The second UNBIND does not indicate an override of the first, and is therefore a duplicate request.

0051
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP, SSP, and EP Messages and Codes* for a complete description.

0052
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP, SSP, and EP Messages and Codes* for a complete description.

0053
An activation request was received for a CDRM whose subarea address is already known by another CDRM name.

0054
An adjacent node is not the node type that the receiving node was configured to expect.

0055
The adjacent node is attempting to establish a connection through a connection network but the virtual routing node CP named in the TG Descriptor (X'46') control vector appended on the received negotiation-proceeding XID3 is not valid.

0056
Locate Phase Error: A Locate GDS variable was received that contained an incorrect request-reply-chain status field; for example, c reply was received while the receiver was in chain state.

0057
The received NOTIFY type is not supported in the current state of the receiver.

0058
An intra-FRSE PVC segment subport received an RNAA (assignment type X'5') with a DLC header link station address field containing a value outside the valid range. The RNAA is rejected.

0059
An intra-FRSE PVC segment subport received an RNAA with a control vector X'43' specifying discontinue link-level contact if an auto network shutdown procedure is initiated. The RNAA is rejected.

005A
RNAA was received to add an intra-FRSE PVC segment subport to a hierarchical physical resource that is not active.

0060
An intra-FRSE PVC segment subport received an RNAA with a control vector X'43' specifying that modem test support is permitted. The RNAA is rejected.

0061
An intra-FRSE PVC segment subport received an RNAA with a control vector X'43' frame send control value field containing a value outside the valid range. The RNAA is rejected.

0062
An intra-FRSE PVC segment subport received an RNAA with a control vector X'43' node type identifier field specifying a node type other than T1. The RNAA is rejected.

0063
An intra-FRSE PVC segment subport received an RNAA with a control vector X'43' specifying that null XID polling for the secondary station should be used. The RNAA is rejected.

0064
A SETCV defining an intra-FRSE PVC segment subport set was received that contained an element address in the DR pool.

0065
A SETCV defining an intra-FRSE PVC segment subport set was received from an SSCP that did not originally add all the subarea element addresses listed in the SETCV to the DR pool.

0066
An ACTTRACE was received for a link connection trace while a trace for a logical link using that link connection was active, or ACTTRACE was received for a logical link trace while a trace for its underlying physical link connection was active.

0067
An intra-FRSE PVC segment subport received an RNAA5 containing a DLC Header Link Station Address that is being used by an existing frame relay terminating equipment subport.

0068
An XID was received with a networking capabilities indicator (specifying whether the sender is an APPN network node) that is not consistent with the receiver definition for the connection. The connection is rejected.

0069
An XID was received with CP services and CP-CP session support indicators that are not consistent with the receiver definition for the connection. The connection is rejected.

006A
A node type mismatch exists between the two SSCPs setting up a VRTG.

VTAM hint: VTAM sets this sense code when a VRTG connection is rejected because the VRTG partner host is configured as an unexpected node type.

006B
The IP address specified in an RNAA(Type=X'05') for a new internet protocol (IP) PU is a duplicate of an existing IP address.

Sense code 080A

Permission rejected: The receiver has denied an implicit or explicit request of the sender; when sent in response to BIND, it implies either that the secondary LU will not notify the SSCP when a BIND can be accepted, or that the SSCP does not recognize the NOTIFY vector key X'0C'. (See the X'0845' sense code for a contrasting response.)

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
An SSCP has denied permission to establish a session through its resources; the receiving SSCP should not attempt to reroute the request to another SSCP.

0002
An SSCP has denied permission to establish a session through its resources; the receiving SSCP should attempt to reroute the request to another SSCP.

0005
The alias application has denied permission to establish a session through this SSCP. The receiving SSCP should not attempt to reroute the request to another SSCP.

0006
The alias application has denied permission to establish a session through this SSCP. The receiving SSCP should attempt to reroute the request to another SSCP.

0007
Permission rejected for an activation request received for a resource that has a network ID different from that of the requesting SSCP, and the requesting SSCP indicated previously that it does not support this configuration.

0008
The request specified in the request change control MS major vector was rejected because it did not originate from a valid focal point.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product.

0009
The request specified in the request change control MS major vector was rejected because the ability to support it has been disabled at the receiver.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product.

000A
The request was rejected because it would prohibit compliance with the status-reporting requirements specified in the reporting level MS common subvector.

000B
The request was rejected because the second-level application, though recognized, operates under the control of a program other than that which has received and is to forward the request to that second-level application program.

000C
The request was rejected because the timer/clock at the receiver is protected and cannot be set by the request sender.

000D
An SSCP or CP has denied a locate search request. The receiving SSCP or CP should attempt to reroute the request.

000E
The request was rejected because of constraints or policies specific to the receiving implementation or installation. The request should not be tried again.

000F
The request was rejected because of constraints or policies specific to the receiving DLUs. The request should not be tried again.

Sense code 080B

Bracket race error: Loss of contention within the bracket protocol. This error can arise when bracket initiation or termination by both NAUs is allowed.

Sense code 080C

Procedure not supported: A procedure (test, trace, IPL, REQMS type, MS major vector key) specified in an RU is not supported by the receiver.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0005
The MS major vector key is not supported by the receiver.

0006
The MS major vector is identified as one that contains a command, but the receiver does not recognize or support the command subvector. (See the X'086C' sense code for the case in which the command subvector is identified, but an additional required subvector is missing.)

0007
Function not supported.

0009
A request for session information retrieval for an independent LU was received in an REQMS; such requests are permitted only in a network management vector transport (NMVT).

000A
A request was received containing a name list or an address list MS subvector with multiple entries, but the receiver supports only a single entry in such a subvector.

000D
An MS request change control major vector was received requesting post-test, but the receiver does not support that function.

000E
An MS request change control major vector was received prohibiting automatic removal of a change, but the receiver does not support that function.

000F
An activate MS major vector was received from a change management focal point specifying use of changes installed in production only, but the receiver supports such a request only when it is received locally.

0012
Application GDS variable in an MDS_MU not supported.

0013
MDS message type not supported. Receiving application does not support the MDS message type in this MDS_MU.

0014
An MS major vector was received requesting execution window timing, but the receiver does not support that function.

0015
An MS activate major vector was received specifying change management activation use, but the receiver does not support that function.

0016
An MS request change control major vector was received requesting activate with force delay, but the receiver does not support that function.

0017
The changes referred to in a request change control MS major vector are already installed on trial and the receiver does not support the transfer from trial to production with REMOVABILITY=YES.

0018
An MS request change control major vector was received requesting pretest, but the receiver does not support that function.

0019
A link trace requested in ACTTRACE is not supported for frame-relay logical links.

0161
Focal point authorization request (X'61') subvector missing the function subfield. (X'10', X'20', or X'30') is required.

0162
Focal point authorization reply (X'62') subvector missing the function subfield. (X'10', X'20', or X'30') is required.

0163
Focal point authorization request (X'63') subvector missing the function subfield. (X'10' or X'30') is required.

0164
Focal point authorization reply (X'64') subvector missing the function subfield. (X'10' or X'20') is required.

4001
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

4003
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

Sense code 080D

NAU contention: A request to activate a session was received while the receiving half-session was awaiting a response to a previously sent activation request for the same session; for example, the SSCP receives an ACTCDRM from the other SSCP before it receives the response for an ACTCDRM that it sent to

the other SSCP, and the SSCP ID in the received ACTCDRM was less than or equal to the SSCP ID in the ACTCDRM previously sent.

Sense code 080E

NAU not authorized: The requesting NAU does not have access to the requested resource.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: A possible cause of this error is that the PLU is not defined or cannot be found.

0001
The PU, according to its system definition, does not accept an ACTPU from any SSCP having the network ID of the sending SSCP.

0002
A gateway T4 node received a request that was not valid from an SSCP that is not in the native network of the gateway node.

0003
The link station received a CONTACT from an unauthorized SSCP.

0004
A BFCLEANUP is received from an unauthorized SSCP.

0005
A RNAA is received from an unauthorized SSCP.

0006
A network node (NN) received a REGISTER from an unauthorized end node.

0007
A network node (NN) received a REGISTER from another network node (NN); receiver rejects the REGISTER with this code.

0008
A network node (NN) received a DELETE from another network node (NN); receiver rejects the DELETE with this code.

0009
A network node (NN) received a DELETE from an unauthorized end node.

000B
A Locate/CD-Initiate was received from a node that is not defined as a client end node. This can be detected by either DS or SS.

000C
A gateway T4 node received a dynamic dump request from an SSCP that is not in the native network of the gateway T4 node.

Sense code 080F

End user not authorized: The requesting end user does not have access to the requested resource.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

0002
Session-level LU-LU verification protocol mismatch: An LU that supports only the enhanced LU-LU verification protocol received a BIND or RSP(BIND) that specified the basic LU-LU verification protocol.

0003
An attempt was made to enter a remote subnetwork to which the origin subnetwork was not authorized.

VTAM Hint: This sense code can be displayed in a VTAM message, but is set by another product.

0004
An attempt was made to install or remove a database table before issuing a logon to the database.

6051
Access security information not valid: The request specifies an access security information field that is not acceptable to the receiver; for security reasons, no further detail about the error is provided. This sense data is sent in FMH-7 or UNBIND.

VTAM hint: A security protocol error has been detected in an RU received from the remote LU or transaction program. For persistent verification, VERIFY and PV must be coded on the conversation security level (CONVSEC) in the RACF® profile.

6052
Authentication failed.

6053
Not signed on.

6054
Lifetime expired.

6055
Authentication required.

6058
Access failure: The request specifies an access security information field that is not acceptable due to a processing failure. This sense code is allowed only on sessions that support extended security sense codes.

8000
Access failure: GSS-API unexpected status value — A GSS-API request returned an unrecognized status value.

8001
Access failure: GSS-API GSS_BAD_MECH — unsupported mechanism requested

8002
Access failure: FSS-API GSS_BAD_NAMETYPE — name of unsupported type provided

8003
Access failure: GSS_API GSS_BAD_BINDINGS — channel binding mismatch

8004
Access failure: GSS_API GSS_BAD_NAME — no valid name provided

8005
Access failure: GSS_API GSS_BAD_STATUS — no valid input status selector

8006
Access failure: GSS_API GSS_BAD_SIG — token had invalid signature

8007
Access failure: GSS_API GSS_DEFECTIVE_CREDENTIAL — defective credential detected

8008
Access failure: GSS_API GSS_DEFECTIVE_TOKEN — defective token detected

8009
Access failure: GSS_API GSS_FAILURE — failure, unspecified at GSS_API level

800A
Access failure: GSS_API GSS_NO_CONTEXT — no valid security context specified

800B
Access failure: GSS_API GSS_NO_CRED — no valid credentials provided

8101
Retryable access failure: GSS_API GSS_CONTEXT_EXPIRED — specified security context expired

8102
Retryable access failure: GSS_API GSS_CREDENTIALS_EXPIRED — expired credentials detected

8103
Retryable access failure: Deferred authentication processing was requested, but communications failures occurred while attempting to communicate with the distributed authentication service TP.

8104
Retryable access failure: Deferred authentication processing was requested, but the origin could not locate the conversation's security context.

FF00
Access failure: The request specifies a password that is expired. This sense code is allowed only on sessions that support extended security sense codes.

FF01
Access failure: The request specifies a password that is invalid. This sense code is allowed only on sessions that support extended security sense codes.

FF02
Access failure: The request specifies a user ID that is revoked. This sense code is allowed only on sessions that support extended security sense codes.

FF03
Access failure: The request specifies a user ID that is invalid. This sense code is allowed only on sessions that support extended security sense codes.

FF04
Access failure: The request is missing a user ID. This sense code is allowed only on sessions that support extended security sense codes.

FF05
Access failure: The request is missing a password. This sense code is allowed only on sessions that support extended security sense codes.

FF06
Access failure: The request specifies a group that is invalid. This sense code is allowed only on sessions that support extended security sense codes.

FF07
Access failure: The request specifies a user ID that is revoked in the specified group. This sense code is allowed only on sessions that support extended security sense codes.

FF08
Access failure: The request specifies a user ID that is not defined in the specified group. This sense code is allowed only on sessions that support extended security sense codes.

FF09
Access failure: The request specifies a user ID that is not authorized to access the remote LU. This sense code is allowed only on sessions that support extended security sense codes.

FF0A
Access failure: The request specifies a user ID that is not authorized to access the remote LU from the local LU. This sense code is allowed only on sessions that support extended security sense codes.

FF0B
Access failure: The request specifies a user ID that is not authorized to access the transaction program at the remote LU. This sense code is allowed only on sessions that support extended security sense codes.

FF0C
Access failure: The request failed due to installation exit processing at the remote LU. This sense code is allowed only on sessions that support extended security sense codes.

FF0D
Access failure: The request failed due to processing failure between the local LU and remote LU. This is a correctable error, so subsequent requests might succeed. This sense code is allowed only on sessions that support extended security sense codes.

Sense code 0810

Missing requester ID: The required requester ID was missing.

Sense code 0811

Break: Asks the receiver of this sense code to terminate the present chain with CANCEL or with an FMD request carrying EC. The half-session sending the break sense code enters chain-purge state when break is sent; the half-session receiving the break sense code discards the terminated chain without ever retransmitting it.

Sense code 0812

Insufficient resources: Receiver cannot act on the request because of a temporary lack of resources.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: A possible cause of this error is that VTAM cannot find a predefined application program definition or model application program definition when processing an OPEN macro for an application program requesting to open its ACB.

0001
More PUs or LUs requested by RNAA than are present in the pool.

VTAM hint: If you are activating a PU connected to an NCP, check the NCP LUDRPOOL definition statement.

See *NCP, SSP, and EP Resource Definition Reference* for more information.

0002
More PUs or LUs are requested by RNAA than the attachment resource will hold.

0003
Resources are not currently available to support an XRF session.

0004
The RNAA request indicates that the requested address must be pre-ENA compatible, but no pre-ENA compatible address is available. See z/OS Communications Server: SNA Resource Definition Reference for information about MAXSUBA.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0005
The requested reserved resources for sessions are not available: In RNAA, a reservation of session resources exceeded those available; no address was assigned and no change was made to the current reservation of the LU.

0006
Insufficient resources are available for a boundary LU-LU session.

VTAM hint:

- For NCP-attached devices, when there is a BIND, INITOTHER or RNAA failure, check the following NCP parameters:
  - NUMILU, NUMTYPE1, and NUMTYPE2 in the LUDRPOOL statement
  - AUXADDR on the BUILD statement
  - The LUPOOL statement, if applicable

  See *NCP, SSP, and EP Resource Definition Reference* for more information.
- Check the system log or the network log for additional messages that might pertain to the problem. For example, if message IST651I is issued for STORAGE UNAVAILABLE BS BUFFER POOL, it might be necessary to increase the size of the buffer pool.

0007
Insufficient resources are available for LU address allocation.

0008
No buffer space: The session was deactivated because of a buffer shortage when extending a nonextended positive RSP(BIND). Insufficient resources exist to extend a BIND response.

0009
No unreserved session connectors are available to add an LU.

000A
A network node does not have adequate resources to honor a Register request (the available directory capacity has already been reached).

000B
A BFSESSINFO was received for an LU that is unknown to VTAM. VTAM attempted to create a representation for the LU, but was unable to do so because of insufficient resources.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

000C
Not enough buffer space exists to support a deadlock-free transmission group. The receiver does not have enough buffers to allocate a BIND receive buffer.

000D
Insufficient buffers exist to activate a session.

000E
The network names table is full.

VTAM hint: The NCP network names table is full. Increase the NNT in the NAMTAB on the BUILD definition statement. This sense code is set by the NCP.

See *NCP, SSP, and EP Resource Definition Reference* for more information.

000F
Insufficient buffer space exists to build a BFINIT.

0010
The CP does not have adequate resources to process a GDS variable request; it will deactivate its CP-CP sessions with the partner CP.

0011
There is insufficient storage available to the SNA component to satisfy the request at this time.

VTAM hint: A possible cause of this error is that VTAM is trying to build a dynamic application program from a model application program definition and there is not enough storage to allow VTAM to build the dynamic application program.

0012
No network address available to assign to a parallel session.

0014
This session has failed because of storage depletion at an intermediate node.

0015
Insufficient resources are available to initiate a short hold mode logical connection.

0016
Unknown network identifier.

0017
Insufficient buffer space exists to process a nonimmediate UNBIND.

0018
All LFSIDs this node is allowed to assign on the TG are in use at this time; the request is rejected.

0019
Insufficient storage is available to conduct an XID exchange.

001A
Insufficient storage is available to activate a TG.

001B
Insufficient resources to activate a token-ring connection.

VTAM hint: A possible correction for this error is to code the NCP parameter NEWDEFN, and the output deck must be supplied to the VTAM configuration found in SYS1.VTAMLST.

See Defining SNA data sets in the z/OS Communications Server: New Function Summary for information about key data sets.

001C
Insufficient storage exists to respond precisely to an error condition.

001D
The PU Type 4 node does not have sufficient disk space to perform the requested dump.

001E
A session has failed because depletion of pooled buffer storage has exceeded a critical threshold resulting from that session monopolizing the usage.

0021
A received XID3 cannot be fully processed because the receiver has insufficient storage to keep the network-qualified name of the control point of the sender.

0022
No specific code applies.

VTAM hint: This sense code can be displayed in a VTAM message but is set by NCP. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a description of sense codes set by NCP.

0023
No specific code applies.

VTAM hint: This sense code can be displayed in a VTAM message but is set by NCP. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a description of sense codes set by NCP.

0024
No specific code applies.

VTAM hint: This sense code can be displayed in a VTAM message but is set by NCP. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a description of sense codes set by NCP.

0025
Insufficient storage to keep the network-qualified name of the connection network virtual node control point.

Sense code 0813

Bracket bid reject—no RTR forthcoming: BID (or BB) was received while the first speaker was in the in-bracket state, or while the first speaker was in the between-brackets state and the first speaker denied permission. RTR will not be sent.

VTAM hint: First speaker refers to the contention winner.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Bracket bid reject: The component was in the in-bracket state when a bracket request was received.

0002
Bracket bid reject: The component was in the between-bracket state when a bracket request was received.

Sense code 0814

Bracket bid reject—RTR forthcoming: BID (or BB) was received while the first speaker was in the in-bracket state, or while the first speaker was in the between-brackets state and the first speaker denied permission. RTR will be sent.

Sense code 0815

Function active: A request to activate a network element or procedure was received, but the element or procedure was already active.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
A session activation request was received by a boundary function to activate a session that was already active.

0002
A session activation request was received by a gateway function to activate a cross-network session that was already active.

0003
Processing for another management services request in progress. Sender should try the request again.

Note: This sense data is sent only by a Type 2 node, which might lack sufficient queuing space.

0004
A bind was received from an T2.1 node when the session receiver rejects the bind.

0005
An IPL function (the loading or storing of a load module) is in progress (MOSS busy).

0006
The short hold mode logical connection selected has been recalled on another port.

0007
A session activation request was received by an APPN node to activate a CP-CP session that was already active.

0009
A session activation request was received by an APPN end node to activate a CP-CP session with a network node when a CP-CP session is already active with another network node.

Sense code 0816

Function inactive: A request to deactivate a network element or procedure was received, but the element or procedure was not active.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000
No specific code applies.

0001
A session deactivation request was received by an APPN node to deactivate a CP-CP session that was not active.

Sense code 0817

Link or link resource inactive: A request requires the use of a link or link resource that is not active.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Link inactive.

VTAM hint: A possible cause of this error is that auto activation is not supported for the PU.

0002
Link station inactive.

0003
Switched link connection inactive.

0004
The TG number of the desired link has been renegotiated to a new value; the route cannot be activated.

0005
Service link inactive.

0006
The link between an SNA node and an attached processor is inactive; for example, the connection between the main processor and its attached service processor goes down.

0007
The requested test was not initiated because the link to be tested was put into an inactive state.

0008
The requested test was interrupted because the link to be tested was put into an inactive state.

0009
Transport configuration table entry not active.

VTAM hint: An APPN host-to-host channel PU is being activated and one of following situations has occurred:

- The resource definition table entry (RDTE) for the transport resource list element (TRLE) whose name is specified in the PU definition cannot be found in the transport resource list (TRL).
- The RDTE for that name is not a transport resource list element.

VTAM fails the activation of the PU and the PU is left in an inactive state.

Perform the following steps:

1. Issue a D NET,ID=*puname* command to determine which TRLE name is specified on the PU definition statement.
2. Issue a D NET,TRL command to get a list of the TRLEs that are defined in the TRL.

If the name specified on the PU definition cannot be found in the list obtained using the D NET,TRL command, verify that the TRLE name is spelled correctly in the PU definition, that the TRLE name exists and is spelled correctly in the TRL definition, and that no other resource has the same name as the TRLE name.

4001
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

Sense code 0818

Link procedure in process: CONTACT, DISCONTACT, IPL, or other link procedure in progress when a conflicting request was received.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

0002
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

0003
CONTACT not serialized, retry: An initial CONTACT procedure is in progress and a nonactivation CONTACT was received by the PU. The nonactivation CONTACT is rejected until the initial CONTACT procedure is completed.

0004
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be an NCP sense code. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a complete description.

0005
Link problem determination test for a modem in progress.

0006
On-line terminal test in progress.

0007
SDLC link test, Level 2, in progress.

0009
The requested test was not initiated because another test was already in progress.

000A
An online terminal test (OLTT) is active on the service link.

000B
SDLC link test, Level 2, in progress on the service link.

000C
Link problem determination test for a modem on the service link in progress.

Sense code 0819

RTR not required: Receiver of ready to receive has nothing to send.

Sense code 081A

Request-sequence error: Sequence of requests not valid.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
An ACTLU was received and no SSCP-PU session exists.

0002
An IPL or DUMP RU sequence error has occurred.

0004
An NC_ER_TEST was to be sent as a result of receiving a ROUTE_TEST request. The ROUTE_TEST was sent in one subnetwork, the NC_ER_TEST was to be sent in another. The SSCP sending the ROUTE_TEST did not have a required alias address within the subnetwork where the NC_ER_TEST was to be sent. (Before sending ROUTE_TEST, the SSCP sends RNAA, or the installation predefines the alias address, so that an origin SSCP address is available within the subnetwork of the route being tested. This address is then specified in the NC_ER_TEST RU.)

0006
RNAA Rejected: If the PU to which the LU is to be added is RNAA added and a control vector has not been received, the RNAA is rejected. A SETCV for the PU has not been received and processed.

0007
A CONTACT, BIND, or ACTLU has been received from an SSCP that has not established ownership of a permanent (system-defined) resource. The resource is not usable until RNAA(Move) has been received.

0008
A CONTACT, BIND, or ACTLU has been received from an SSCP that has not established ownership of a temporary (DR added) resource. The resource is not usable until RNAA(ADD) has been received.

0009
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product.

000F
Set aside for implementation-specific use, and will not be otherwise defined in SNA; see implementation documentation for details of usage.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product.

0010
The request is rejected or fails because the entry point or a target resource in the entry point is already in the state or condition that the request would have produced.

0011
A CONTACT was received specifying APPN in its connection support field, but was not preceded by a CONNOUT, a protocol violation.

0012
A CONTACT was received with a connection support field value that does not match that in the preceding CONNOUT.

0013
A CONNOUT, specifying LEN in its connection support field, was received for a nonswitched link station, a protocol violation.

0014
A CONTACT was received for an intra-FRSE PVC segment subport whose frame-relay port is in a discontacted state. The CONTACT is rejected.

0015
A CONTACT was received for an RNAA-added intra-FRSE PVC segment subport and a SETCV with a FRSE (X'80') control vector has not been received. The CONTACT is rejected.

Sense code 081B

Receiver in transmit mode (a race condition): Normal-flow request received while the half-duplex contention state was not-receive, (*S,¬R), or while resources (such as buffers) necessary for handling normal-flow data were unavailable. (Contrast this sense code with sense code X'2004', which signals a protocol violation.)

Sense code 081C

Request not executable: The requested function cannot be executed, because of a permanent error condition in the receiver.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

Note: For VTAM sense codes, the meaning of the data in bytes 2 and 3 is dependent upon the context of the sense code.

0000
No specific code applies.

0002
The receiver has an error resulting from a software problem that prevents execution of the request.

0004
For request dump request units:

A requested NCP dump has been terminated because of a permanent I/O error on the dump file—the dump is partially complete and can be formatted and printed.

For activate link and deactivate link request units:

During activation of a channel link, the channel device name for the link to be activated did not consist of three valid hexadecimal digits.

0008
For request load (conditional) and request load (unconditional) request units:

VTAM is unable to successfully open the data set containing the NCP load module.

For request dump request units:

A requested NCP dump has been terminated because of a permanent communication controller I/O error—the dump is partially complete and can be formatted and printed.

For activate link and deactivate link request units:

During activation of a channel link, the channel device name for the link to be activated was found not to have been defined to the operating system.

0009
Device is not online due to system action or explicit system operator action. The device must be varied online. Contact the system operator.

000C
For request load (conditional) and request load (unconditional) request units:

One of the following situations has occurred:

- A permanent I/O error has occurred on the diagnostic or load-module data set.
- The diagnostic program has detected a probable communication controller hardware error.
- A permanent I/O error has occurred on the communication controller. Check that the channel adapter is enabled and that the device is attached.

For Request dump request units:

A requested NCP dump has been terminated because of a permanent I/O error on the dump file—the dump data set cannot be formatted and printed.

For activate link and deactivate link request units:

The hardware device type associated with the channel device name of the channel link being activated is not supported by the PU receiving an ACTLINK.

0010
For request load (conditional) and request load (unconditional) request units:

A time-out has occurred while the diagnostic load program was running (hardstop in the communication controller).

For request dump request units:

A requested NCP dump has been terminated because of a permanent communication controller I/O error—the dump data set cannot be formatted and printed.

For activate link and deactivate link request units:

During activation of a channel link, the attached device specified by a channel device name could not be allocated because it was already allocated to another user.

VTAM hint:

- This sense code can occur in response to a VARY ACT command for an NCP if U=*device_numbers* is specified on the command when the same device number has already been activated.
- When this sense code is received in message IST380I for an ACTLINK request, message IST1386I might also be issued. See the return code and reason code in IST1386I to determine the cause of the failure.

0014
For request load (conditional) and request load (unconditional) request units:

The loaded NCP has encountered an error, preventing successful initialization.

For request dump request units:

Cannot successfully open the dump data set.

0018
For request load (conditional) and request load (unconditional) request units:

Load not performed—HALT is in progress.

001C
For request load (conditional) and request load (unconditional) request units:

The communication controller dump-load-restart router has received an input work element that contains an unrecognized command code. The NCP load module is not present in the load module data set (BLDL failure).

This error might also occur if there is an I/O error while loading the file.

0020

For request load (conditional) and request load (unconditional) request units:

A permanent I/O error has occurred. Possible reasons include, but are not limited to, the following ones:

- The device type is not defined properly.
- The communication controller is not in the proper state for loading.
- The service processor is not in the proper state. For example, MOSS-E is powered off.
- A hardware error occurred.
- The channel adapter address in NCP GEN might not match the hardware address.

For request dump request units:

Unable to successfully load a necessary dump utility module, or insufficient storage is available.

For activate link and deactivate link request units:

VPBUF storage is insufficient.

0024

For request load (conditional) and request load (unconditional) request units:

VTAM is unable to successfully open the data set containing the diagnostic program (ddname INITTEST).

0028

For request load (conditional) and request load (unconditional) request units:

A load of an NCP was requested with an SSP release prior to V3R4 and a release of VTAM prior to V3R2 (this is prohibited), or IFWLEVEL was not loaded with SSP V3R4.

For activate link and deactivate link request units:

During deactivation of a channel link, a device could not be deallocated by the operating system.

For request dump request units:

A requested NCP dump has been terminated because ENQUEUE of the dump data set failed—DASD was not opened and the dump data set cannot be formatted and printed.

002C

For request load (conditional) and request load (unconditional) request units:

The diagnostic program has detected a probable communication controller hardware error.

0030

For request load (conditional) and request load (unconditional) request units:

The NCP or diagnostic program load module has a block size greater than 1024 bytes (the DC option was not specified when the link edit was performed), or the channel adapter address of the controller is not correct in NCP GEN.

For activate link and deactivate link request units:

During activation of a channel link, the operating system path validation failed for the device specified by the channel device name.

0034

For activate link and deactivate link request units:

An SSCP sent ACTLINK or DACTLINK for a resource type to which ACTLINK or DACTLINK does not apply.

0038

For activate link and deactivate link request units:

During activation or deactivation of a channel link, the RDTE was not found, causing a permanent error in locating the resource definition was detected in the PU.

If this sense code is issued as the result of the activation of a 3172 XCA major node, verify that the ADAPNO parameter on the PORT definition statement matches the adapter number assigned by the IBM 3172 communication controller.

If this sense code is issued as the result of the activation of an XCA major node used in conjunction with an Open Systems Adapter, verify that the ADAPNO parameter on the PORT matches the adapter number configured in the OSA, and that the MEDIUM parameter on the PORT matches the media type that the OSA is configured to support.

003C

For request load (conditional) and request load (unconditional) request units:

The communication controller unit control block does not contain a valid value for the channel-adapter-type field, or the channel adapter address of the controller is not correct in NCP GEN.

For activate link and deactivate link request units:

During activation of a channel link, the device specified by the channel device name was found not to have been made available by the operating system.

0040

For request load (conditional) and request load (unconditional) request units:

The NCP or diagnostic program load module is improperly constructed.

For activate link and deactivate link request units:

During activation of a channel link, the operating system could not complete OPEN processing, denying access to the channel link.

For request dump request units:

A requested NCP dump has been terminated because the dump file is empty.

0044

For request load (conditional) and request load (unconditional) request units:

The IFLOADRN communication controller load utility program is unable to allocate sufficient storage.

0048

For request load (conditional) and request load (unconditional) request units:

The function is already active; the NCP is already loaded.

004A

For request load (conditional) and request load (unconditional) request units:

The NCP is ready to receive the load module.

004C

For request load (conditional) and request load (unconditional) request units:

The size of the NCP load module exceeds the storage capacity of the communication controller.

0050

For request load (conditional) and request load (unconditional) request units:

A permanent I/O error has occurred on the NCP load-module library.

0054

For request load (conditional) and request load (unconditional) request units:

A permanent I/O error has occurred on the diagnostic program load-module library (ddname INITTEST).

0058

For request load (conditional) and request load (unconditional) request units:

A diagnostic program cannot be located in the diagnostic program load-module library (ddname INITTEST)—BLDL failure.

005C

For request load (conditional) and request load (unconditional) request units:

Request Load (conditional) is attempted while another host is already loading the communication controller (unit exception on SENSE channel program).

0060

For request load (conditional) and request load (unconditional) request units:

Start I/O condition Code 3 on SENSE channel program can occur for the following reasons:

- Request load (conditional) is attempted while another host is already loading the communication controller.
- Channel bypass switch is on.
- If the request load is attempted through an ESCON channel, check the fiber link for loose connectors.

0064

For request load (conditional) and request load (unconditional) request units:

A load I/O operation (to a link-attached communication controller) has been purged (by VARY INACT or error recovery of the communication controller of another node in the path to the communication controller).

0068

For request load (conditional) and request load (unconditional) request units:

A load I/O operation (to a link-attached communication controller) has failed (a negative response has been generated by the adjacent communication controller).

0070

For request load (conditional) and request load (unconditional) request units:

A load from the disk was initiated, and the save was ignored.

0074

For request load (conditional) and request load (unconditional) request units:

Error caused by specifying DIAG with the 3725 or the 3720.

0078

For request load (conditional) and request load (unconditional) request units:

Either the CCU is not at the correct level, or the CTLR disk option is not available.

007C

For request load (conditional) and request load (unconditional) request units:

Load module not available on disk.

0080

For request load (conditional) and request load (unconditional) request units:

MOSS error–load module not loaded from the disk.

0084

For request load (conditional) and request load (unconditional) request units:

MOSS error–load module and switch not saved.

0088

For request load (conditional) and request load (unconditional) request units:

The disk function is not supported. Either the CCU is not the correct level, or the CTLR disk option is not available.

008C
For request load (conditional) and request load (unconditional) request units:

The NCP load module has an entry point address of zero.

0090
For request load (conditional) and request load (unconditional) request units:

Warning–loading continued: cannot perform LOADFROM, SAVEMOD, or DUMPLOAD.

00AB
For request load (conditional) and request load (unconditional) request units:

Load not performed—the load subtask has abended.

For request dump request units:

Dump not performed—the dump subtask has abended.

00B0
For request load (conditional) and request load (unconditional) request units:

Probable MOSS error—the load module or switch might not be saved.

00B4
For request load (conditional) and request load (unconditional) request units:

MOSS error–switch not saved.

00B8
For request load (conditional) and request load (unconditional) request units:

Load already in progress.

00BC
For request load (conditional) and request load (unconditional) request units:

Duplicate load module on the disk.

00C0
For request load (conditional) and request load (unconditional) request units:

No room on the disk.

00C4
For request load (conditional) and request load (unconditional) request units:

A disk resource is temporarily unavailable.

00C8
For request load (conditional) and request load (unconditional) request units:

RU length error.

00CC
For request load (conditional) and request load (unconditional) request units:

The request was cancelled by the operator.

00D0
For request load (conditional) and request load (unconditional) request units:

A fast load was not performed, a sequential load has been started.

00D4
For request load (conditional) and request load (unconditional) request units:

The logical unit block (LUB) for the controller is not valid.

00D8
For request load (conditional) and request load (unconditional) request units:

The scheduled IPL cannot be cancelled because it was never scheduled.

00DC

For request load (conditional) and request load (unconditional) request units:

The function is not supported.

00E0

For request load (conditional) and request load (unconditional) request units:

RU sequence error.

00E4

For request load (conditional) and request load (unconditional) request units:

Another load module has been scheduled to IPL within five minutes on the MOSS disk.

00E8

A request was made to BINDER to perform the GETBUF function. The request failed with the return code specified in the message.

00EC

A request was made to BINDER to perform the STARTD function. The request failed with the return code and reason code specified in the message.

00F0

A request was made to BINDER to perform the CREATEW function. The request failed with the return code and reason code specified in the message.

00F2

For request load (conditional) and request load (unconditional) request units:

IPL time is earlier than the system time.

00F4

A request was made to BINDER to perform the INCLUDE function. The request failed with the return code and reason code specified in the message.

00F6

For request load (conditional) and request load (unconditional) request units:

Notify time is earlier than the system time.

00F8

A request was made to BINDER to perform the GETDATA function. The request failed with the GETDATA function. The request failed with the message.

00FC

A request was made to BINDER to perform the FREEBUF function. The request failed with the return code specified in the message.

0A01

An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status has not changed from the state previous to the execution. Volatile storage error.

0A02

An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status has not changed from the state previous to the execution. Nonvolatile storage error.

0A03

An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status has not changed from the state previous to the execution. Link connection component interface error.

0A04
An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status has not changed from the state previous to the execution. Unspecified software error condition.

0B01
An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status was modified from the state existing previous to the execution. Volatile storage error.

0B02
An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status was modified from the state existing previous to the execution. Nonvolatile storage error.

0B03
An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status was modified from the state existing previous to the execution. Link connection component interface error.

0B04
An error was detected by the DLC manager of the receiving node during the execution of a management services request. The link connection status was modified from the state existing previous to the execution. Unspecified software error condition.

Sense code 081D

network address or name not valid: A node, station, or CP identifier in the request was not valid.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
The station ID or SSCP ID in the request was not valid.

0001
The network ID, LU name pair in the request was not valid.

0002
Resource name found in the request was not valid.

0003
The network ID, SSCP name pair in the request was not valid.

0004
A duplicate CP name has been detected, causing the links to one or both nodes to be deactivated.

VTAM hint: If a PU will always be used as a LEN node, CONNTYPE=LEN should be specified on the PU definition statement.

Sense code 081E

Session reference error: The request contained reference to a half-session that either could not be found or was not in the expected state (generally applies to network services requests).

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: A possible cause of this error is that the ACTCDRM was sent to the incorrect network in the gateway NCP.

0001
No session found: The session identified in the BFCLEANUP was not found; the BFCLEANUP is rejected.

0002
The session identified in the BFCINIT was not found; the BFCINIT is rejected.

0003
No session was found during the processing of a session services request.

0004
The appropriate session was found during processing of a session services request, but the session is not in the expected state.

Sense code 0820

Control vector error: Data for the control vector specified by the target network address and key was not valid.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: If this sense code is set in response to a SETCV RU, then the MAXOUT value is incorrect. It must be between one and 127, or equal to one or 127.

0001
In a SETCV defining an intra-FRSE PVC subport set, one or both of the primary subport partners that define the subport set are not defined.

0002
In a SETCV defining an intra-FRSE PVC subport set, a specified element address does not define a subport within a subport set, or is defined more than once in a subport set.

0003
An element address of an intra-FRSE PVC subport set received in a SETCV was found to be already associated with another subport set.

Sense code 0821

Session parameters not valid: Session parameters included on a BIND were not valid or not supported by the half-session whose activation was requested. The session parameters are usually obtained from the logmode table entry.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- Sessions cannot log on to CICS.

  If this problem occurs, the sense code is displayed in message IST663I, and *request* is **CINIT**. When running CICS with AUTO-INSTALLATION, the terminal definition in the terminal control table terminal entry (TCTTE) must match the VTAM LOGMODE definition statement for the device. See the information about common subarea network problems in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this problem.
- The PLU has rejected the BIND session parameters.
- The cryptographic function referenced in the logmode table entry is not active in all SSCPs involved in establishing the session.

0001
Mode name at LU not valid: The specified mode name was not recognized by the LU.

0002
Mode name at CP not valid: The specified mode name was not recognized by the CP.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- A logon mode name was not specified when using dynamic reconfiguration to add a logical unit.

- The logon mode name associated with the session request was not found in the specified mode table or in the default logon mode table (ISTINCLM).

  Verify that the requested logon mode name is defined in the following places:

  – In a subarea environment, the mode name must be defined in the SSCP of the secondary logical unit (SLU).
  – In an APPN environment, the mode name must be defined in the origin and destination nodes, as well as the servers of the origin and destination nodes (if the origin and/or destination is owned by an end node).
  – In a combined APPN and subarea environment, the mode name must be defined at the APPN node that owns the origin or destination, the server of that node (if it is an end node), and at the interchange node(s) that represents the subarea entry points.

    If the SLU is owned by a subarea node other than the interchange node representing the subarea entry point, the mode name must also be defined there.

  because mode table names are not carried on APPN line flows, a user-defined mode table is used only at the SSCP of the SLU. Other nodes defining the mode must define it in the default logon mode table. See z/OS Communications Server: SNA Network Implementation Guide for information about mode-to-class-of-service (COS) resolution in an APPN or combined APPN and subarea environments.

0003
The primary half-session requires cryptography, but the secondary half-session does not support cryptography.

0004
The secondary half-session requires cryptography, but the primary half-session does not support cryptography.

0005
Selective or required cryptography is specified, but no SLU cryptographic data key is provided.

0006
The BIND was rejected because it was non-negotiable and specified a primary send pacing window size larger than the SSCP or boundary function (BF) can handle, as determined by the logon mode entry or PACING/VPACING parameters.

0007
The specified mode name was not recognized in a subarea network.

000A
Specified mode table name not found at receiving CP.

VTAM hint: This sense code indicates that the mode table associated with the LU was not found. Verify that the specified table exists and activate it if necessary.

000B
The PLU requires message authentication code support, but it cannot be supported.

000C
The SLU requires message authentication code support, but it cannot be supported.

000D
The PLU requires Triple-DES but the SLU can provide only DES encryption.

000E
The SLU requires Triple-DES but the PLU can provide only DES encryption. The processor where the PLU is running does not have the Triple-DES chip installed.

Sense code 0822

Link procedure failure: A link-level procedure has failed because of link equipment failure, loss of contact with a link station, or a response to a link command was not valid. This is not a path error, because the request being rejected was delivered to its destination.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies

VTAM hint: Ensure that you have activated the correct line.

0001
The controller is not loaded, but it is ready to receive a load module.

0010
Product-specific sense code.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product.

80nn
nn is product-specific and will not be otherwise defined in SNA.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. It might be issued by NCP. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a description of sense codes set by NCP.

Sense code 0823

Unknown control vector: The control vector specified by a network address and key is not known to the receiver.

Sense code 0824

Logical unit of work abnormally terminated: The current unit of work has been abnormally terminated; when sync point protocols are in use, both sync point managers are to revert to the previously committed sync point.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
For LU 6.2, backout initiated: A transaction program or its LU has initiated backout. The protected resources for the distributed logical unit of work are to be restored to the previously committed sync point. This sense data is sent only in FMH-7.

For non-LU 6.2, no specific code applies.

0001
For LU 6.2, backout initiated: Resync In Progress: A transaction program or its LU has initiated backout. The protected resources for the distributed logical unit of work are to be restored to the previously committed sync point.

When sent in reply to a PS header, resync in progress means that one or more resources in the transaction subordinate to the backout sender have experienced failure so it is not known whether they have backed out.

Sense code 0825

Component not available: The LU component (a device indicated by an FM header) is not available.

Sense code 0826

FM function not supported: A function requested in an FMD RU is not supported by the receiver.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

Sense code 0827

Intermittent error—retry requested: An error at the receiver caused an RU to be lost. The error is not permanent, and retry of the RU (or chain) is requested.

Sense code 0828

Reply not allowed: A request requires a normal-flow reply, but the outbound data flow for this half-session is quiesced or shut down, and there is no delayed reply capability.

Sense code 0829

Change direction required: A request requires a normal-flow reply, but the half-duplex flip-flop state (of the receiver of the request) is not-send, and change direction (CD) was not set on the request. Therefore, there is no delayed reply capability.

Sense code 082A

Presentation space alteration: Presentation space altered by the end user while the half-duplex state was not-send, (¬S,*R); request executed.

Sense code 082B

Presentation space integrity lost: Presentation space integrity lost (for example, cleared or changed) because of a transient condition, for example, because of a transient hardware error or an end-user action such as allowing presentation services to be used by the SSCP.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies

0001
Presentation space violation

Note: The end-user action described under sense codes X'082A' and X'084A' is excluded here.

Sense code 082C

Resource-sharing limit reached: The request received from an SSCP was to activate a half-session, a link, or a procedure, when that resource was at its share limit.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: A possible cause of this error is that the line you are attempting to activate is already active to another SSCP.

0001
Request not valid: The specified link station has already received a CONTACT and is therefore under the control of another SSCP. This CONTACT would exceed the share limit (=1).

0002
Request not valid: The specified PU has already received an ACTPU and is therefore under the control of another SSCP. This ACTPU exceeds the share limit of 1.

VTAM hint: This sense code is for an ACTPU request which is not valid and is issued when the PU is already active. It is set by the dependent LU requester (DLUR). When VTAM receives this sense code on the ACTPU response, it deactivates the PU and fails the VARY DIAL or DIAL START command.

Sense code 082D

LU busy: The LU resources needed to process the request are being used; for example, the LU resources needed to process the request received from the SSCP are being used for the LU-LU session.

Sense code 082E

Intervention required at LU subsidiary device: A condition requiring intervention, such as out of paper, or power-off, or cover interlock open, exists at a subsidiary device.

Sense code 082F

Request not executable because of LU subsidiary device: The requested function cannot be executed, because of a permanent error condition in one or more of the receiver's subsidiary devices.

Sense code 0830

Session-related identifier not found: The receiver could not find a session-related identifier for a specified session.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0001
PCID not found for the specified resources.

0002
LSID not found for the specified session.

Sense code 0831

LU component disconnected: An LU component is not available because of power off or some other disconnecting condition.

Sense code 0832

Count field not valid: A count field contained in the request indicates a value too long or too short to be interpreted by the receiver, or the count field is inconsistent with the length of the remaining fields.

nnnn
Bytes 2 and 3 contain a binary count that indexes (zero-origin) the first byte of the count field that is not valid.

Note: This sense code is not used for a BIND error because the displacement of fields within the BIND might not be the same at both ends of a session when the BIND was affected by name transformations, for example, after the BIND has passed through a gateway. Sense code X'0835' is used to specify a displacement for a BIND error.

Sense code 0833

Parameter (with pointer and complemented byte) not valid: One or more parameters contained in fixed- or variable-length fields of the request are not valid or not supported by the NAU that received the request.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

nnmm
Byte 2 contains a binary value that indexes (zero-origin) the first byte of the parameter that is not valid.

Byte 3 contains a transform of the first byte that contained a parameter that was not valid. The bits that constitute the parameters that are not valid are complemented, and all other bits are copied.

Note: This sense code is not used for a BIND error because the displacement of fields within the BIND might not be the same at both ends of a session when the BIND was affected by name transformations,

for example, after the BIND has passed through a gateway. Sense code X'0835' is used to specify a displacement for a BIND error.

Sense code 0834

RPO not initiated: A power-off procedure for the specified node was not initiated because one or more other SSCPS have contacted the node, or because a contact, dump, IPL, or discontact procedure is in progress for that node.

Sense code 0835

Parameter (with pointer only) not valid: The request contained a fixed- or variable-length field whose contents are not valid or not supported by the NAU that received the request.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

000A
The SLU maximum RU size is not valid.

000B
The PLU maximum RU size is not valid.

nnnn
Bytes 2 and 3 contain a two-byte binary count that indexes (zero-origin) the first byte of the fixed- or variable-length field that has contents that are not valid.

Note: This sense code is not used to report a value that is not valid in an MS major vector. If the value that is not valid occurs in a formatted MS subvector, sense code X'086B' is used. If it occurs in an unformatted subvector, sense code X'0870' is used.

VTAM hint: Sense code 083500*nn* indicates that the BIND contains parameters that are not valid and supplies an index (*nn*) into the BIND that identifies the bytes that the BIND receiver cannot interpret. A buffer trace can provide more problem determination information.

Note: The offset seen in the buffer trace might differ from the offset seen in the IST663I message group and seen by the application.

See the information about common subarea network problems in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this problem.

Sense code 0836

PLU/SLU specification mismatch: For a specified LU-LU session, both LUs are either only primary session capable, or only secondary session capable. A session cannot be established between these two LUs.

Sense code 0837

Queuing limit exceeded: For an LU-LU session initiation request (INIT, CDINIT, or INIT-OTHER-CD), specifying (1) initiate or queue (if initiate not possible) or (2) queue only, the queuing limit of either the OLU or the DLU, or both, was exceeded.

VTAM hint: A possible cause of this error is that the value of MAXSUBA is not consistent throughout the network.

Sense code 0838

Request not executable because of resource or component state incompatibility: The request is not executable because it is not compatible with the state of a resource or component in the receiver.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
The sender has sent valid data. The data parses correctly, but the receiver is in the wrong state to process it because it is not what was expected.

For example, in focal point function, the entry point sends a X'63' subvector, but the focal point incorrectly sends back a X'62' subvector rather than a X'64' subvector. The receiver does not expect the X'62' subvector and cannot process it.

0001
The change referred to in a request change control MS major vector or report-FS-action command cannot be deleted or replaced because it is installed marked removable.

0002
One or more of the changes referred to in a request change control MS major vector cannot be installed, removed, or accepted because they are in back-level state.

0003
One or more of the changes referred to in a request change control MS major vector cannot be installed marked on-trial because they are already installed marked on-trial.

0004
One or more of the changes referred to in a request change control MS major vector cannot be installed marked on-trial or in-production because they are already installed marked in-production removably. They can, however, be accepted if desired.

0005
One or more of the changes referred to in a request change control MS major vector cannot be installed marked on-trial or in-production because they are already installed marked in-production and nonremovable. The only possibility is to perform data object renewal using send-and-install with removability prohibited or desired—but not required.

0006
One or more of the changes referred to in a request change control MS major vector cannot be removed or accepted because they are installed marked nonremovable

0007
One or more of the changes referred to in a request change control MS major vector cannot be removed or accepted because they are not installed.

0008
Pretest is not applicable to one or more of the changes referred to in a request change control MS major vector.

0009
Execution window timing is not applicable to one or more of the changes referred to in a request change control MS major vector.

000A
Automatic removal is not applicable to one or more of the changes referred to in a request change control MS major vector.

000B
Post-test is not applicable to one or more of the changes referred to in a request change control MS major vector.

000D
One or more of the changes referred to in a request change control MS major vector cannot be installed marked in-production because they are installed marked on-trial with a set of corequisites different from those requested on this install request.

000E
One or more of the changes referred to in a request change control MS major vector cannot be accepted because they are installed marked on-trial.

000F
One or more of the changes referred to in a request change control MS major vector or report-FS-action command cannot be replaced or deleted because they are critical system components that must always have an installed instance. The only possibility is to perform data object renewal using send-and-install with removability prohibited or desired—but not required.

0010
One or more of the changes referred to in a request change control MS major vector or report-FS-action command cannot be stored or installed because an implementation-defined limit on the number of changes has been exceeded.

0011
One or more of the changes referred to in a request change control MS major vector or report-FS-action command cannot be deleted or replaced because they are required in order to maintain removability of other changes. They might be in backup state or installed marked in-production.

0012
One or more of the corequisite changes referred to in a request change control MS major vector are missing or are in a state incompatible with the request.

0013
The change referred to in a request change control MS major vector or report-FS-action command cannot be replaced because it is installed marked in-production and non-removable and another change is not being installed in this operation.

0014
One or more of the changes referred to in a request change control MS major vector cannot be installed because a precluded combination of values in the removability, automatic removal, automatic acceptance, or activation use subfields was specified.

0015
One or more of the changes referred to in a request change control MS major vector cannot be installed because one or more changes already installed are still removable for one or more components to be altered by these changes.

0016
One or more of the changes referred to in a request change control MS major vector or report-FS-action command cannot be replaced because they would be required for removable installation, and removability is required.

0017
Execution of the request referred to in an MS cancel major vector has proceeded too far to cancel.

0039
Queuing not supported

003A
The requested function cannot be completed because the specified adjacent node CP capabilities GDS variable does not indicate support for the complementary function.

VTAM hint: This error will occur if you attempt to manually activate CP-CP sessions over an active APPN connection with an adjacent CP that does not support manual activation of CP-CP sessions over active APPN connections. To activate CP-CP sessions with the adjacent CP, you should first deactivate the APPN connection and then reactivate it.

Sense code 0839

LU-LU session being taken down or LU being deactivated.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
During session-initiation processing, a session-termination request has caused the LU-LU session to be taken down.

0002
RNAA (Type 3) received for a session during the process of session deactivation. The RNAA should be tried again.

0003
SSCP detected that this session should no longer exist and requested its termination. For example, BFSESSINFO was received, reporting a subject LU address that the SSCP believed already belonged to a cross domain resource.

Sense code 083A

LU not enabled: At the time an LU-LU session initiation request is received at the SSCP, at least one of the two LUs, though having an active session with its SSCP, is not ready to accept CINIT or BIND requests.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The PLU is not enabled.

0002
The SLU is not enabled.

Sense code 083B

PCID not valid: The received PCID for a new session duplicated the PCID assigned to another session, or the received PCID intended as an identifier for an existing session could not be associated with such an existing session, or an error was detected in the format of the received PCID.

VTAM hint: PCID stands for procedure correlation identifier.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The PCID contained in CDINIT(Initiate or Queue), INIT-OTHER-CD, or CDTAKED duplicates a PCID received previously in one of these requests.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: This error can occur during an attempt to take over a switched connection because a connection-network-capable control point (CP) on the connection network does not have a complete system definition. See the information about common APPN problems in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this session takeover problem.

0002
The received fully qualified PCID duplicated one assigned to another session.

VTAM hint: PCID means procedure-correlation identifier.

When VTAM receives an ACTPU.RSP(-) with this sense code, VTAM will delete the old PCID, then resend the ACTPU request with the newly-generated PCID.
A bind path has looped. For more information, see z/OS Communications Server: SNA Network Implementation Guide.

0003
The received fully qualified PCID contains a network-qualified CP name identical to that of the receiving node.

0004
The received fully qualified PCID duplicated one assigned to another route setup procedure.

0005
The fully qualified PCID received in BFCINIT is not assigned to an existing route setup procedure. The BFCINIT is rejected.

0006
The fully qualified PCID received in BFCLEANUP is not assigned to an existing route setup procedure. The BFCLEANUP is rejected.

Sense code 083C

Domain-takedown contention: While waiting for a response to a CDTAKED, a CDTAKED request is received by the SSCP containing the SSCP-SSCP primary half-session. Contention is resolved by giving preference to the CDTAKED sent by the primary half-session.

Sense code 083D

Dequeue retry unsuccessful—removed from queue: The SSCP cannot successfully honor a CDINIT(dequeue) request (which specifies "leave on queue if dequeue-retry is unsuccessful") to dequeue and process a previously queued CDINIT request (for example, because the LU in its domain is still not available for the specified session), and removes the queued CDINIT request from its queue.

Sense code 083E

Session key 08 required.

0000
No specific code applies.

0001
The implementation-defined limit on XID exchanges was exceeded before link activation completed.

0002
The implementation-defined limit on XID exchanges was exceeded before a nonactivation exchange completed.

0004
The implementation-defined limit on contention-winner CP-CP session activation attempts has been exceeded.

Sense code 083F

Terminate contention: While waiting for a response to a CDTERM, a CDTERM is received by the SSCP of the SLU. Contention is resolved by giving preference to the CDTERM sent by the SSCP of the SLU.

Sense code 0840

Procedure not valid for resource: The named RU is not supported in the receiver for this type of resource. For example, (1) SETCV specifies boundary function support for a Type 1 node, but the capability is not supported by the receiving node or (2) the NCP PU receiving an EXECTEST or TESTMODE is not the primary NCP PU for the target link.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Surrogate session setup failed.

0002
Link cannot be used because it supports only HPR routing and the session requires non-HPR routing.

VTAM hint: A possible cause of this error is that a session request was received from an adjacent VTAM subarea node by a VTAM APPN node that supports only HPR routing, such as a VTAM node that communicates in native mode across an asynchronous transfer mode (ATM) network.

0003
Link not valid: The link to which the PU is to be added is not an SNA link. Only SNA links are supported.

0004
Link not valid: A request that is allowed only for a nonswitched link was received for a link that is defined to the receiver as switched.

0005
Resource was not dynamically added: This request works only with resources that were added through dynamic reconfiguration.

0007
Resource not found: A DELETE or FIND could not be satisfied because the specified entry does not exist in the receiving directory.

VTAM hint:

- VTAM cannot find a model definition to build a dynamic application program when the dynamic application program requests to open its ACB.
- VTAM cannot find a dynamic application program when the dynamic application program requests to close its ACB.

0008
The directory entry cannot be deleted. The network node received a DELETE with a delete entry condition indicating that the entry can be deleted only if it is a leaf. The entry is not a leaf; therefore, the DELETE is rejected.

0009
RNAA(Move) received a resource that was added through dynamic reconfiguration. Such a resource may not be moved through RNAA(Move).

000A
Procedure invalid for resource: A PN supporting independent LUs has dialed into a boundary function that does not support sessions with independent LUs. The SSCP cannot activate the independent LUs.

000B
The REGISTER request specifies that a unique directory entry is required (for example, the REGISTER is for an LU), but there is a duplicate in the directory data base.

0010
A SETCV with control vector X'43' has been received for a nonswitched resource.

0011
A dynamically added or switched resource has not yet been activated.

0012
A request was received that is allowed only for a primary link station. The request must utilize the service link and that link is defined as secondary.

0013
A CONNOUT request was received that contained an invalid X.21 call type.

0014
A CONNOUT or CONTACT was received specifying that the receiver is to designate itself as an APPN end node in XID3s that it sends to an attached APPN or LEN.

0015
This sense data value is generated whenever an APPN session route must be calculated in two pieces (using two separate RSCVs) and it is determined that the two RSCVs identify a common node; that is, the session route passes through a given node twice.

0016
This sense data value is generated whenever an RSCV is precalculated because the OLU or DLU was thought to be in a subarea network and it is determined (based on the RSCV) that the location of the DLU is incorrect; that is, the RSCV indicates that the DLU is in the APPN network, but the DLU is really in a subarea network, or vice versa.

0017
A session initiation request was received for a multinode persistent enabled application program with a precalculated RSCV, but no HPR connection can be set up using the precalculated route.

VTAM Information: The Locate is resubmitted and the RSCV recalculated using a set of tail vectors that VTAM supplies on the Locate reply.

VTAM hint: The error occurred because a VTAM V4R2 or VTAM V4R1 node calculated the RSCV.

Sense code 0841

Duplicate network address: In an LU-LU session initiation request, one of the specified LUs has a duplicate network address already in use. This error can be caused by a mismatch between the CDRM and NCP gateway NAU subarea/element definitions.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
The SSCP of the DLU determines that the OLU network address specified in the CDINIT request is a duplicate of an LU network address assigned to a different LU name.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0001
A duplicate SLU address is found during session initiation.

0002
A duplicate PLU address is found during session initiation.

0003
An SSCP finds a duplicate network address for the DLU on the OLU side of the gateway.

0004
An SSCP finds a duplicate network address for the DLU on the DLU side of the gateway.

0005
An SSCP finds a duplicate network address for the OLU on the OLU side of the gateway.

0006
An SSCP finds a duplicate network address for the OLU on the DLU side of the gateway.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- A gateway NCP freed a network address before VTAM is finished with it. To diagnose the problem, first identify which LU has the network address and determine why NCP thinks it is freed. This will require looking at both a VTAM dump and a VTAM internal trace. Find the failing SRTA in the trace; it usually precedes the CPRC. From there, you can identify the LU. Most likely, there will be a SIB queued to the LU. This will provide some information about why the network address is still in use.
- There is a mismatch between the VTAM CDRM definitions for a null network attached user and the user gateway NCP GWNAU statements.

  For example, this VTAM has a CDRM definition for ADJNETEL=2, but the user gateway NCP does not have a GWNAU statement for ELEMENT=2. The problem is intermittent because the gateway NCP assigns element numbers randomly.
- There are gateway NCPs sharing the same subarea in the same null network.

0008
An ACTCDRM request was received that contained a network address already in use.

Sense code 0842

Session not active.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: The SSCP-SSCP session, which is required for the processing of a network services request, is not active. For example, at the time an LU-LU session initiation or termination request is received, at least one of the following conditions exists:

- The SSCP of the ILU and the SSCP of the OLU do not have an active session with each other, and therefore, INIT-OTHER-CD cannot flow.
- There is no active session between two specific SSCPs in the session setup path. RUs cannot be routed from one SSCP directly to the other SSCP. However, other SSCPs may be tried.

Note: This value is used if there is not enough data to select one of the more specific codes listed below.

0001
The session between Type 2.1 CPs is not active.

0002
For a session-initiation request, an SSCP does not have an SSCP-SSCP session with an SSCP in the direction of the DLU.

0003
For a session-initiation request, an SSCP does not have an SSCP-SSCP session with an SSCP in the direction of the OLU.

0004
An intermediate SSCP has lost connectivity with an SSCP in the session setup path for an LU-LU session. This sense data is used when the SSCP previously lost connectivity with one or more participating gateway nodes so that it cannot learn that the LU-LU session is ended by receiving a NOTIFY RU from a gateway node.

FFFF
Logon intercepted.

Sense code 0843

Required synchronization not supplied: For example, a secondary LU (LU Type 2 or 3) received a request with write control code = start print, along with RQE and ¬CD.

Sense code 0844

Initiation dequeue contention: While waiting for a response to a CDINIT(dequeue), a CDINIT(dequeue) is received by the SSCP of the SLU. Contention is resolved by giving preference to the CDINIT(dequeue) sent by the SSCP of the SLU.

Sense code 0845

Permission rejected—SSCP will be notified: The receiver has denied an implicit or explicit request of the sender; when sent in response to BIND, it implies that the secondary LU will notify the SSCP (via NOTIFY vector key X'0C') when a BIND can be accepted, and the SSCP of the SLU supports the notification. (See sense code X'080A' for a contrasting response.)

Sense code 0846

ERP message forthcoming: The received request was rejected for a reason to be specified in a forthcoming request.

Sense code 0847

Restart mismatch: Sent in response to STSN, SDT, or BIND to indicate that the secondary half-session is trying to execute a resynchronizing restart but has received insufficient or incorrect information.

Sense code 0848

Cryptography function inoperative: The receiver of a request was not able to decipher the request because of a malfunction in its cryptography facility.

Sense code 0849

System generation mismatch.

VTAM hint: If an ACTLINK fails with this sense code for an Enterprise Extender line, it means that inconsistent DYNPU values are specified on the Enterprise Extender groups that meet the following conditions:

- These groups are all call-in capable.
- These groups are all associated with the same static VIPA (IPADDR).
- These groups are not associated with a virtual routing node. In other words, VNNAME is not specified.

Sense code 084A

Presentation space alteration: The presentation space was altered by the end user while the half-duplex state was not-send, (¬S,*R); request not executed.

Sense code 084B

Requested resources not available: Resources named in the request, and required to honor it, are not currently available. It is not known when the resources will be made available.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: This error can be caused by a DR ADD for a duplicate address. Check your DR statements to see if an address was duplicated.

0001
BIND queuing not supported, retry: The SLU is not available and the sender of the UNBIND does not support BIND queuing as requested by the PLU.

0002
Requested resource not available: For dynamic reconfiguration MOVE, ADD, or ADDLINK operation, the requested local address is already assigned to an active resource. For MOVE PU, this is the DLC address; for MOVE LU, the LU local address.

0003
The application transaction program specified in the request is not available.

0004
Session resources unavailable: The receiver of the RNAA cannot satisfy the request for reserved session resources specified on the assign LU characteristics (X'30') control vector.

VTAM hint: A possible cause of this error is a mismatch between the values specified on the EAS and MAXSESS operands on the BUILD definition statement.

0005
Controller resource is not available.

0009
The intersubnetwork Locate failed because the maximum number of intersubnetwork hops was exceeded. The value of the maximum intersubnetwork hop count field in the locate was reduced by a number greater than one while being processed by a border node along the route.

6002
The resource identified by the destination program name (DPN) is not supported.

6003
The resource identified by the primary resource name (PRN) is not supported.

6031
Transaction program not available, retry allowed: The FMH-5 attach command specifies a transaction program that the receiver is unable to start. Either the program is not authorized to run or the resources to run it are not available at this time. The condition is temporary. The sender is responsible for subsequent retry. This sense data is sent only in FMH-7.

Sense code 084C

Permanent insufficient resource: Receiver cannot act on the request because resources required to honor the request are permanently unavailable. The sender should not try again immediately because the situation is not transient. This error can occur if MAXBFRU is either not read because of a coding error or not coded.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
For LU 6.2, transaction program not available, no retry: The FMH-5 Attach command specifies a transaction program that the receiver is unable to start. The condition is not temporary. The sender should not try again immediately. This sense data is sent only in FMH-7.

For non-LU 6.2, no additional information is specified.

0001
Request not processed: Processing an ACTLINK request, and read buffers not allowed. The ACTLINK request will not be processed.

0002
Creating allocation exception: The receiver is unable to create the specified data object as a result of an insufficient storage condition that occurred at allocation time.

0003
Replacing allocation exception: The receiver is unable to replace the specified data object as a result of an insufficient storage condition that occurred at allocation time.

0006
Data-object storing exception: The receiver is unable to store the specified data object as a result of an insufficient storage condition that occurred during the storing process.

0007
Data-object classification code not supported: The receiver is unable to satisfy the allocation requirements of the specified data-object classification code.

0008
Volume not mounted: The receiver is unable to perform the requested allocation/storing operation because the required volume is not mounted.

hnnn
Where $h \geq 8$; that is, the high-order bit in Byte 2 is set to one. The 15 low-order bits of Bytes 2 and 3 contain a binary count that indexes (zero-origin) the first byte of the field found to be in error.

Sense code 084D

Session parameters not valid—BF: The session parameters were not valid or were unacceptable by the boundary function.

Sense code 084E

Session parameters not valid—PRI: A positive response to an activation request (for example, BIND) was received and was changed to a negative response because session parameters that were not valid were carried in the response. The services manager receiving the response sends a deactivation request for the corresponding session. This error can occur if NETIDs are coded incorrectly on any NETWORK

statements in CDRM definitions. See z/OS Communications Server: SNA Resource Definition Reference for more information.

Sense code 084F

Resource not available: A requested resource is not available to service the given request.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The disk is full; therefore, the load module cannot be stored.

0002
The security component is not available.

Sense code 0850

Link-level operation cannot be performed: An IPL, dump, or remote power off (RPO) cannot be performed through the addressed link station because the system definition or current state of the hardware configuration does not allow it.

0000
No specific code applies.

0001
Link activation limit reached: The specified TG was not activated because the maximum number of active link stations allowed on this port has already been reached.

Sense code 0851

Session busy: Another session that is needed to complete the function being requested on this session is temporarily unavailable.

VTAM hint: A possible cause of this error is that the session needed by the host to complete the command is busy.

Sense code 0852

Duplicate session activation request: Two session activation requests have been received with related identifiers. The relationship of the identifiers and the resultant action varies by request.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint:

- If the RU is an ACTPU or ACTCDRM, it means that a session has already been activated for the subject destination-origin pair by a session activation request that carried a larger activation request identifier than the current request; the current request is refused.
- If the RU is an ACTLU, a session has already been activated for the subject destination-origin pair by a session activation request. The current request is denied.
- If the RU is a BIND, it means that the BIND request was received with the same session-instance identifier (in the structured subfield X'03' of the user data field) as an active session's; the current request is refused.

0001
Received a second BIND from a peripheral node PLU while the session is still in the activation process.

0002
A REQACTPU has been received by an SSCP that has already sent an ACTPU for the same PU.

Sense code 0853

TERMINATE(Cleanup) required: The SSCP cannot process the termination request, as it requires cross-domain SSCP-SSCP services that are not available. (The corresponding SSCP-SSCP session is not active.) TERMINATE(Cleanup) is required.

Sense code 0855

Route Setup procedure failure: An intermediate or destination node was unable to successfully complete the processing of a high-performance routing (HPR) Route Setup request or reply.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000
No specific code applies.

0001
The destination LU is not ready to accept sessions.

0002
An unknown destination LU was specified in the request.

0003
A TG specified in the RSCV could not be activated.

0004
An unknown TG was specified in the RSCV.

0005
A TG specified in the RSCV has failed.

0006
A TG specified in the RSCV was not activated as an HPR TG.

0007
An intermediate node had insufficient storage to activate a TG specified in the RSCV.

0008
The receiving node had insufficient storage to process the route setup request.

0009
The route setup request was received over a TG that was not activated as an HPR TG.

000A
A VR within a composite network node is inoperative.

000B
The receiving node does not support HPR protocols.

000C
The receiving node does not support the HPR transport option.

000D
The route setup request or reply could not be forwarded over the TG in the FID2 format because its size was greater than the TG maximum BTU size.

000E
The value of the current hop count field of the RSCV received in a route setup request exceeded the value of the destination hop index field in the request (for example, the route setup request appeared to have passed the destination node).

000F
The route setup request completed unsuccessfully. The route setup reply was not received in the allotted time (as determined by the IOPURGE start option).

0020
The intended destination was not able to perform the RTP function (for example, it does not support the RTP transport tower). When a negative route setup reply with this sense code passes through an RTP-capable intermediate node, the intermediate node attempts to become the new destination and perform the RTP function.

VTAM hint: This might be encountered due to an error in the definition of an activate-on-demand switched link, which was dialed as the result of the route setup request. If the link was predefined as HPR capable, but the partner node does not support HPR (or does not wish to support HPR protocols on the designated link), the route setup will fail when the link fails to activate as an HPR-capable link.

This should not lead to a failure to set up the session, but might lead to the use of normal APPN intermediate session routing instead of HPR.

0021
An extended border node rejected a path switch attempt due to locally defined restrictions that do not allow RTPs to pass through that node. This sense code could be set during APPN Locate search processing or route setup processing for an RTP connection that is undergoing path switch. For APPN Locate search processing, this sense code might not cause a search failure. Rather, this sense code causes APPN Locate search processing to continue, thereby allowing discovery of alternate paths to the target node, which support the path switching RTP.

Sense code 0856

SSCP-SSCP session lost: Carried in the sense data field in a NOTIFY (third-party notification vector, X'03') or -RSP(INIT_OTHER) sent to an ILU to indicate that the activation of the LU-LU session is uncertain because the SSCP(ILU)-SSCP(OLU) session has been lost. (Another sense code, X'0842', is used when it is known that the LU-LU session activation cannot be completed.)

Sense code 0857

SSCP-LU Session Not Active: The SSCP-LU session, required for the processing of a request, is not active; for example, in processing REQECHO, the SSCP did not have an active session with the target LU named in the REQECHO RU.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

VTAM hint: The primary logical unit (PLU) or secondary logical unit (SLU) is not available.

0001
The SSCP-SLU session is in the process of being reactivated.

0002
The SSCP-PLU session is inactive.

VTAM hint: For a USERVAR, an APPL or CDRSC definition with the same name as the USERVAR was found and was not active.

0003
The SSCP-SLU session is inactive.

VTAM hint: For independent logical units, the independent logical unit is inactive.

0004
The SSCP-PLU session is in the process of being reactivated.

0005
The SSCP lost connectivity with the PLU after the LU-LU session was started, and has no other way to learn that the session has ended; the SSCP either never had a session to a gateway node in the LU-LU session path, or had previously lost connectivity to it.

0006
The SSCP lost connectivity with the SLU after the LU-LU session was started, and has no other way to learn that the session has ended; the SSCP either never had a session to a gateway node in the LU-LU session path, or had previously lost connectivity to it.

0007
The selected ALS for the OLU is not in a state permitting LU-LU sessions to be established using it. The condition is detected when the session request (BFINIT) was received, but, when the request was processed, the ALS was no longer in an active state. The session request is rejected.

0008
The selected ALS for the DLU is not in a state permitting LU-LU sessions to be established using it. The condition is detected when the session request was being processed in the DLU domain and the ALS selected for the DLU is no longer in an active state. The session request is rejected.

Sense code 0858

SSCP-SSCP session activation rejected.

0000
No specific code applies.

0001
An SSCP rejected a received ACTCDRM attempting to restart a session that terminated as a result of an operator-initiated nondisruptive deactivation request.

VTAM hint: This is not an error condition. The ACTCDRM was rejected because the SSCP that was deactivated is at a prior level of VTAM.

Sense code 0859

REQECHO data-length error: The specified length of data to be echoed (in REQECHO) violates the maximum RU size limit for the target LU.

Sense code 085A

Specific server exception: an architecturally defined or customer-defined server that is sensitive to data object contents has detected an exception.

Sense code 085B

Unknown resource name: the identified resource, required to complete the requested unit-of-work, is not known to the SNA node.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Unknown server name. When this SNA report code is used in an SNA condition report, it is accompanied by a supplemental report containing the server name.

0002
Unknown agent.

0003
The clock identifier specified in an MS set clock major vector is unknown to the receiver.

0004
The timing source name specified in an MS set clock major vector is unknown to the receiver.

0005
The agent unit-of-work correlator referred to by an MS cancel major vector is unknown to the receiver, or represents a unit of work already completed.

Sense code 085C

System exception: the node experiences an exception condition within a resident system or subsystem that inhibits subsequent processing by the SNA component.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The exception is identifiable as a system-related problem.

0002
The exception is identifiable as a permanent system-related problem.

Sense code 085D

The MU_id could not be accepted in the MU_id registry.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The MU_id is a duplicate. When this SNA-Report-Code is used in an SNA_Condition_Report, it is accompanied by three supplemental-reports that identify information about the receiver MU_id registry: supplemental-report 1 contains the lowest MU_id the receiver would accept; supplemental-report 2 contains the highest MU_id the receiver would accept; supplemental-report 3 contains the time stamp of the receiver's MU_id registry.

0002
The MU_id value is greater than expected. When this SNA-Report-Code is used in an SNA_Condition_Report, it is accompanied by three supplemental-reports that identify information about the receiver's MU_id registry: supplemental-report 1 contains the lowest MU_id the receiver would accept; supplemental-report 2 contains the highest MU_id the receiver would accept; supplemental-report 3 contains the time stamp of the receiver's MU_id registry.

0003
A temporary condition prevents acceptance of the MU_id.

0004
A permanent condition prevents acceptance of the MU_id.

0005
The MU_id registry is not initialized.

Sense code 085E

Operator intervention.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The operator has suspended the transmission of the message unit.

0002
The operator has purged the message unit.

Sense code 0860

Function not supported—continue session: The function requested is not supported; the function might have been specified by a request code or some other field, control character, or graphic character in an RU.

nnnn
Bytes 2 and 3 contain a two-byte binary count that indexes (zero-origin) the first byte in which an error was detected. This sense code is used to request that the session continue, thereby ignoring the error.

Sense code 0861

COS name not valid: The class-of-service (COS) name, either specified by the ILU or generated by the SSCP of the SLU from the mode table is not in the "COS name to VR identifier list" table used by the SSCP of the PLU.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
COS name was generated by the SSCP.

VTAM hint: If this sense code is displayed in message IST663I, and message IST264I follows, this might indicate that an incorrect COS table is referenced. The NetView program also has a COS table, and if this error occurs, the NetView program library was concatenated in front of the VTAM library causing the wrong table selection. See the information about common subarea network problems in z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this problem.

0001
COS name was generated by the ILU.

0002
The COS name generated by the Type 2.1 CP local to, or the Type 2.1 NNCP server for, the ILU is not in the COS name definition table.

0003
The CDINIT request or response contains a session initiation control vector that has class-of-service (COS) name fields that have not been properly specified. A virtual route list could not be found associated with the COS name.

Sense code 0862

Medium presentation space recovery: An error has occurred on the current presentation space. Recovery consists of restarting at the top of the current presentation space. The sequence number returned is of the RU, in effect, at the top of the current presentation space.

nnnn
Bytes 2 and 3 following the sense code contain the byte offset from the beginning of the RU to the first byte of the RU that is displayed at the top of the current presentation space.

Sense code 0863

Referenced local character set identifier (LCID) not found: A referenced character set does not exist.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

hnnn
Where *h*≥8; that is, the high-order bit in byte 2 is set to one. The 15 low-order bits of bytes 2 and 3 contain a binary count that indexes (zero-origin) the first byte of the field found to be in error.

Sense code 0864

Function terminated abnormally: The conversation was terminated abnormally. Other terminations might occur after repeated reexecutions; the request sender is responsible for detecting such a loop.

VTAM hint: Sense codes in the X'0864*nnnn*' range should not be used with APPCCMD CONTROL=SEND,QUALIFY=ERROR,TYPE=USER unless followed by an APPCCMD CONTROL=DEALLOCATE macro. These codes indicate to the receiver that deallocation is occurring.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000

For LU 6.2, premature conversation termination: The conversation is terminated abnormally; for example, the transaction program might have issued a DEALLOCATE_ABEND verb, or the program might have terminated (normally or abnormally) without explicitly terminating the conversation. This sense data is sent only in FMH-7 or UNBIND.

For LU 6.2 half-duplex conversations, this sense data is sent only in FMH-7 or indicated in UNBIND.

For LU 6.2 full-duplex conversations, this sense data is also sent in the negative response that precedes an FMH-7, when there is a chain to respond to. The sense data in the negative response gives advance notice to the transaction program (in the form of an error return code) that an ERP message is forthcoming. For this error, the ERP message will contain the same sense data value used in the negative response.

For non-LU 6.2, no additional information is specified.

0001

System logic error—no retry: A system logic error has been detected. No retry of the conversation should be attempted. This sense data is sent only in FMH-7 or UNBIND.

For LU 6.2 half-duplex conversations, this sense data is sent only in FMH-7 or indicated in UNBIND.

For LU 6.2 full-duplex conversations, this sense data is also sent in the negative response that precedes an FMH-7, when there is a chain to respond to. The sense data in the negative response gives advance notice to the transaction program (in the form of an error return code) that an ERP message is forthcoming. For this error, the ERP message will contain the same sense data value used in the negative response.

0002

Excessive elapsed time—no retry: Excessive time has elapsed while waiting for a required action or event. For example, a transaction program has failed to issue a conversation-related protocol boundary verb. No retry of the conversation should be attempted. This sense data is sent in UNBIND when there is no chain to respond to; otherwise, it is sent in FMH-7.

For LU 6.2 half-duplex conversations, this sense data is sent in UNBIND when there is no chain to respond to; otherwise, it is sent in FMH-7.

For LU 6.2 full-duplex conversations, this sense data is also sent in the negative response that precedes an FMH-7. The sense data in the negative response gives advance notice to the transaction program (in the form of an error return code) that an ERP message is forthcoming. For this error, the ERP message will contain the same sense data value used in the negative response.

0003

Allocation error message forthcoming: An error has been detected in a received attach request, resulting in a rejection of the attach. The sense data value that indicates the reason for rejection will be specified in a forthcoming FMH-7.

This sense data is sent in the negative response that precedes an allocation error FMH-7 for an LU 6.2 full-duplex conversation. The negative response gives advance notice to the transaction program (in the form of an error return code) that an ERP message is forthcoming.

Note: The phrases following the sense data are symbolic return codes provided to a full-duplex transaction program when a negative response with sense data is received by the LU. (See *SNA Transaction Programmer's Reference Manual for LU 6.2* for full-duplex verbs and possible return codes.)

Sense Data
Return Code

08640000
ERROR_INDICATION (with a subcode of DEALLOCATE_ABEND_PROG)

08640001
ERROR_INDICATION (with a subcode of DEALLOCATE_ABEND_SVC)

08640002
ERROR_INDICATION (with a subcode of DEALLOCATE_ABEND_TIMER)

08640003
ERROR_INDICATION (with a subcode of ALLOCATION_ERROR)

Sense code 0867

Sync event response: Indicates a required negative response to an (RQE,CD) synchronizing request.

Sense code 0868

No panels loaded: Referenced format not found because no panels are loaded for the display.

Sense code 0869

Panel not loaded: The referenced panel is not loaded for the display.

Sense code 086A

Subfield key not valid: A subfield key in an MS subvector was not valid in the conditions under which it was processed.

nnmm
Byte 2 following the sense code contains the subvector key (*nn*) of the subvector containing the unrecognized subfield, and byte 3 contains the unidentified subfield key (*mm*).

Sense code 086B

Subfield value not valid: A value in a subfield within an MS major vector is not valid for the receiver.

nnmm
Byte 2 following the sense code contains the subvector key (*nn*) of the subvector containing the subfield with the value that was not valid, and byte 3 contains the subfield key (*mm*) of the subfield with the invalid value.

Note: See sense code X'0870' for the case in which the invalid value occurs in an unformatted subvector, that is, one not containing subfields with keys and lengths, or in the unformatted portion of a partially formatted subvector.

6991
Dial information error

ATM
ATM dial information does not indicate ATMSVC or SHARE/EXCLUSIVE.

VTAM hint: A possible cause of this error is that the values ATMSVC or SHARE or EXCLUSIVE might be missing or could be specified incorrectly on the DLCADDR operand (subfield 1) on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH statement in the switched major node.

EE
A mismatch of IP address families has been detected. See message IST1891I for specific information about the error.

6997
ATM traffic description is not valid.

VTAM hint: A possible cause of this error is that the best effort indicator, cell rates, and traffic management options might be missing or could be specified incorrectly on the DLCADDR operand (subfield 7) on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

6998
ATM quality of service (QoS) class is not valid.

VTAM hint: A possible cause of this error is that the quality of service (QoS) class might be missing or could be specified incorrectly on the DLCADDR operand (subfield 8) on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

6999
ATM transit network selection (TNS) identifier is not a valid length.

VTAM hint: A possible cause of this error is that the carrier identification code might be missing or could be specified incorrectly on the DLCADDR operand (subfield 9) on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

69A5
ATM addresses are not a valid length or type.

VTAM hint: A possible cause of this error is that the ATM address or addresses might be missing or could be specified incorrectly on the DLCADDR operand (subfield 21) on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

69C3
ATM bearer capabilities are not specified or are specified incorrectly.

VTAM hint: A possible cause of this error is that the ATM bearer capabilities are not specified or are specified incorrectly on the DLCADDR operand (subfield 51) on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

69CD
ATM adaptation layer is not specified or is specified incorrectly.

VTAM hint: A possible cause of this error is that the ATM adaptation layer is not specified or is specified incorrectly on the DLCADDR operand (subfield 61) on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

Sense code 086C

Required control vector or subvector missing: One or more control vectors or MS subvectors that are required by the receiver to perform some function are missing from the received message, or are not present in the required position.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

nn00
Byte 2 following the sense code contains the key (nn) of one of the control vectors or subvectors that is missing, or improperly positioned. Byte 3 is reserved (00).

Note: See the X'080C0006' sense data for the case in which the major vector key is recognized but a subvector representing the function to be performed cannot be identified.

0400
Subvector X'04' not first.

0800
Reported on destination prefix (X'08') subvector not present.

0900
Reported on destination location (X'09') subvector not present.

0B00
Reported on destination suffix (X'0B') subvector not present.

2100
Required focal point identification (X'21') subvector not present. Already found either X'61', X'63', or X'E1' subvector.

4400
Second CV in TDU was not a CV44.

4600
CV46 not present.

7D00
Report code (X'7D') subvector not present.

8000
First CV in TDU was not a GVC280.

8100
Origin location name (X'81') subvector not present.

8200
Destination location name (X'82') subvector not present.

9000
Flags (X'90') subvector not present.

Sense code 086D

Required subfield missing: A control vector or MS subvector lacks one or more subfield keys required by the receiver to perform the function requested.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

nnmm
Byte 2 following the sense code contains the key (nn) of the subvector or control vector lacking a required subfield, and byte 3 contains the subfield key (mm) of a missing subfield.

0901
NETID (X'01') subfield of the reported on destination location (X'09') subvector not present.

0902
NAU (X'02') subfield of the reported on destination location (X'09') subvector not present.

2101
Focal point identification (X'21') subvector is missing the MS_category subfield (X'01').

2102
Focal point identification (X'21') subvector is missing the flags subfield (X'02').

2110
Focal point identification (X'21') subvector is missing the FP netid subfield (X'10').

2111
Focal point identification (X'21') subvector is missing the FP NAU name subfield (X'11').

2112
Focal point identification (X'21') subvector is missing the FP application program name subfield (X'12').

2120
Focal point identification (X'21') subvector is missing the backup FP netid subfield (X'20') when either the backup FP NAU name (X'21') subfield or the backup FP application program name (X'22') subfield was found.

2121
Focal point identification (X'21') subvector is missing the backup FP NAU name subfield (X'21') when the backup FP Netid (X'20') subfield is present.

2122
Focal point identification (X'21') subvector is missing the backup FP application program (X'22') subfield when the backup FP netid (X'20') subfield and the backup FP NAU name (X'21') subfield are present.

4580
Node characteristics (X'45') control vector is missing the node type and status subfield (X'80').

4680
TG descriptor (X'46') control vector is missing the TG identifier subfield (X'80').

6240
Focal point authorization reply (X'62') subvector missing current FP CP-name subfield (X'40') when required for the authorization request rejected (X'20') subfield or the authorization revoked (X'30') subfield.

6241
Focal point authorization reply (X'62') subvector missing current FP application program subfield (X'41') when required for the authorization request rejected (X'20') subfield or the authorization revoked (X'30') subfield.

6991
ATM dial information indicating ATMSVC or the type of SVC that can be used is not specified.

VTAM hint: A possible cause of this error is that the DLCADDR operand (subfield 1) on the following definition statements in the following major nodes is not coded:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

6997
ATM traffic description is not specified.

VTAM hint: A possible cause of this error is that the DLCADDR operand (subfield 7) on the following definition statements in the following major nodes is not coded:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

69A5
No ATM dial information is specified when a dial operation is attempted through a native ATM network.

VTAM hint: A possible cause of this error is that the DLCADDR operand (subfield 21) on the following definition statements in the following major nodes is not coded:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

8101
NETID (X'01') subfield of the origin location name (X'81') subvector not present.

8102
NAU name (X'02') subfield of the origin location name (X'81') subvector not present.

8103
MS application program name (X'03') subfield of the origin location name (X'81') subvector not present.

8201
NETID (X'01') subfield of the destination location name (X'82') subvector not present.

8202
NAU name (X'02') subfield of the destination location name (X'82') subvector not present.

8203
MS application program name (X'03') subfield of the destination location name (X'82') subvector not present.

Sense code 086E

Subvector combination not valid: Two or more subvectors, each permissible by itself, are present in a combination that is not allowed.

nnmm
Bytes 2 and 3 following the sense code contain the subvector keys (*nn*) and (*mm*) of two of the subvectors that should not be jointly present.

Sense code 086F

Length error: A length field within an MS major vector is not valid, or two or more length fields are incompatible.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The MS major vector length is incompatible with the RU length.

0002
The sum of the MS subvector lengths is incompatible with the MS major vector length.

0007
The length field of an MDS_MU is incompatible with the sum of the lengths of the imbedded GDS variables, or a length that was not valid was found in an imbedded structure (or GDS variable).

0008
The length field of a CP-MSU is incompatible with the sum of the lengths of the imbedded structures.

000A
The length field of a route setup GDS variable is incompatible with the sum of the lengths of the imbedded structures.

000B
The sum of the control vector lengths in an RU or XID is incompatible with the length of the RU or XID.

2103
The sum of the subfield lengths in the focal point identification (X'21') subvector incompatible with the length of the subvector.

2106
One or more of the subfields in focal point identification (X'21') subvector has an invalid length field.

8103
The sum of the subfield lengths in the origin location name (X'81') subvector is incompatible with the length of the subvector.

8106
The origin location name (X'81') subvector of the MDS routing information (X'1311') GDS variable contains an invalid subfield length. (This is specified only if the sum of the subfield lengths is compatible with the subvector length).

8203
The sum of the subfield lengths in the destination name (X'82') subvector is incompatible with the length of the subvector.

8206
The destination location name (X'82') subvector of the MDS routing information (X'1311') GDS variable contains an invalid subfield length. (This is specified only if the sum of the subfield lengths is compatible with the subvector length).

9005
The flags (X'90') subvector length is invalid in the MDS routing information (X'1311') GDS variable. (The length is not five.)

***nn*03**
The sum of the subfield lengths in an MS subvector is incompatible with the subvector length. Byte 2 following the sense code contains the subvector key.

***nn*05**
The MS subvector length is not valid. Byte 2 following the sense code contains the relevant subvector key (*nn*). (This is specified only if the sum of the subvector lengths is compatible with the major vector length.)

***nn*06**
The Subfield length is not valid. Byte 2 following the sense code contains the subvector key (*nn*) of the MS subvector containing the invalid subfield length. (This is specified only if the sum of the subfield lengths is compatible with the subvector length.)

***nn*09**
The sum of the subfield lengths in a control vector is incompatible with the control vector length. Byte 2 following the sense code contains the control vector key.

***nn*0C**
The length field of a control vector in an RU or XID is not valid. Byte 2 following the sense code contains the control vector key.

Sense code 0870

Unformatted subvector value invalid: A value in an unformatted MS subvector, or in an unformatted portion of a partially formatted MS subvector, is not valid.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

nnxx
Byte 2 following the sense code contains the subvector key (nn) of the MS subvector containing the value that is not valid. Byte 3 contains a one-byte binary count that indexes the first byte in which the invalid value falls. The indexing is zero-origin, from the beginning of the subvector.

Note: See sense code X'086B' for the case in which the value that is not valid occurs in a formatted MS subvector, that is, one containing subfields with keys and lengths, or in the formatted portion of a partially formatted subvector.

8106
Subfield length in origin location name not valid(X'81') subvector. NETID is not a valid length (1-8 characters).

8206
Subfield length in destination location name not valid(X'82') subvector. NETID is not a valid length (1-8 characters).

9002
Flags (X'90') subvector contains setting that is not valid for MDS message type.

9003
Flags (X'90') subvector contains an flag setting that is not valid.

Sense code 0871

Read partition state error: A read partition structured field was received while the display was in the retry state.

Sense code 0872

Orderly deactivation refused: An NC_DACTVR(Orderly) request has been received, but sessions are assigned to the VR and it will not be deactivated.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
An NC_DACTVR(Orderly) request has been received, but sessions are assigned to the VR and it will not be deactivated.

0001
An MS major vector specifying orderly deactivation of the receiving node has been received, but sessions are active and their implied deactivation is not allowed; the requested activation will not proceed.

0002
An MS major vector specifying deactivation of the receiving node has been received, but the receiver cannot determine if sessions are active; the requested activation will not proceed.

Sense code 0873

Virtual route not defined: No ERN is designated to support this VRN.

Sense code 0874

ER not in a valid state: The ER supporting the requested VR is not in a state allowing VR activation.

Sense code 0875

Incorrect or undefined explicit route requested: The reverse ERNs specified in the NC_ACTVR do not contain the ERN defined to be used for the VR requested, or the ERN designated to be used for the VR is not defined.

Sense code 0876

Nonreversible explicit route requested: The ERN used by the NC_ACTVR does not use the same sequence of transmission groups (in reverse order) as the ERN that should be used for the RSP(NC_ACTVR).

Sense code 0877

Resource mismatch: The receiver of a request has detected a mismatch between two of the following resources: (1) its definition of an affected resource, (2) the actual configuration, and (3) the definition of the resource as implied in the request.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Link defined as switched is nonswitched: A link defined to an ACTLINK receiver as being switched was found to be nonswitched during the activation attempt.

0002
Link defined as SDLC is non-SDLC: A link defined to an ACTLINK receiver as being SDLC was found to be non-SDLC during the activation attempt.

0003
Link defined as having automatic connect-out capability does not: A link defined to an ACTLINK receiver as having automatic connect-out capability was found to lack it during the activation attempt.

0004
ACTLINK received for a resource other than a link: An ACTLINK was received that resolved to a local device number representing a device other than a link.

0005
Link defined as X.21 is not X.21.

0006
Link defined as LPDA-capable is configured in NRZI mode.

0007
A request that is allowed only for a primary link station was received for a link station that is defined to the receiver as secondary.

0008
A request for link problem determination for modems was received for a link that is defined to the receiver as not supporting link problem determination for modems.

0009
A request for link problem determination for modems was received for a link that is defined to the receiver as a supporting link, but no problem determination support for modems was found on the link.

000A
A request that is allowed only for a nonswitched link was received for a link that is defined to the receiver as switched.

000B
A request that is allowed only for a link with a modem not using the multiplexed links feature was received for a link that is defined to the receiver as having a modem using the multiplexed links feature.

000C
Resource definition mismatch for modems: A request that is allowed only for a link with a nontailed modem was received for a link that is defined to the receiver as having a tailed modem.

000D
The sending SSCP and the receiving Type 4 node having conflicting system definitions. A BIND has been received for an SLU that contains an incorrect SLU address. The LU address in the BIND is a primary address. The LU address cannot be used for a secondary role on a new session.

000E
The sending SSCP and the receiving Type 4 node have conflicting system definitions. A BIND has been received for an independent LU, but the LU specified is not in a Type 2.1 node.

000F
The sending SSCP and the receiving Type 4 node have conflicting system definitions. The SSCP owner is the same as the SSCP sending the nonactivation CONTACT PIU but the PU is not a Type 2.1. The CONTACT is for a Type 2.1 node, but the PU is not defined as Type 2.1 to the receiver.

0010
The BFCLEANUP is for an independent LU, but the LU specified is not an independent LU.

0011
The subarea address portion of an addressed LU is not equal to the subarea address of the Type 4 node. The LU is not in the same subarea as the Type 4 node.

0012
If the BFCLEANUP is for a resource that is not a BF LU, the request will be rejected. This is a situation where the function is not supported by the target resource. It can be caused by a SYSDEF mismatch between the Type 4 node and the SSCP.

0013
The network ID field in the BIND SLU name is not equal to the network ID of the boundary function, or the SLU name field is not equal to the LU name field in the boundary function control block for the LU.

0014
The LU specified in the FNA is not associated with the PU specified in the FNA; that is, an LU address (byte 7–*n*) is not associated with the PU target address specified.

0015
BFCINIT name mismatch: The BIND cannot be built from the BFCINIT because the NQ PLU name does not match. The session activation is rejected by the boundary function with a BFTERM.

0016
Invalid target address; either:

- The PU with which the specified LUs are to be associated is not Type 1 or Type 2; that is, the SSCP attempts to add an LU to a PU, but the boundary function has defined that PU as a Type 4.
- The SSCP sent an RNAA assignment Type X'0' or X'5' with a PU or LU specified instead of a link. This is caused by a definition mismatch.

0017
MAXSUBA required for pre-ENA address assignment: If MAXSUBA is not specified and an RNAA requesting a pre-ENA address is received, the RNAA is rejected.

0018
An RNAA Type 4 was received requesting an auxiliary address on a dependent LU.

0019
Multiple sets of dial information are specified for a native ATM call when only one set is allowed.

VTAM hint: A possible cause of this error is that more than one DLCADDR operand (subfield 1 or 21) is specified on the following definition statements in the following major nodes:

- GROUP definition statement in the XCA major node (TGs to connection networks)
- PATH definition statement in the switched major node (TGs over SVCs)

001A
The target LU specified in a BFCLEANUP or BFCINIT is not associated with the same link station that is associated with the session indicated in the URC control vector.

001B
The target link station specified in a BFCLEANUP is not the same link station as the session indicated in the URC control vector.

001C
Resource definition mismatch for BFCINIT: The sending SSCP and the receiving Type 4 node have conflicting system definition. A BFCINIT has been received for an LU address that is currently being used by an active LU-LU session. The LU address is primary on this already active session. The LU address cannot be used for a secondary role on a new session.

001D
The LU address in the BFCINIT is a secondary address; the BFCINIT is rejected.

001E
The subject LU specified in the BFSESSINFO RU is not defined to the SSCP as an independent LU; this is a mismatch between the SSCP and the BF.

001F
A dependent LU is attached to a PU that indicates ACTPU is to be suppressed; the SSCP cannot activate the LU because ACTLU is not supported.

VTAM hint: The PU sent an XID that had the ACTPU suppression bit turned on. You need to reconfigure the PU to correct the error.

0020
A peripheral node supporting independent LUs has attached (using a nonswitched link) to a Type 2 PU that cannot have independent LU sessions through it. The SSCP activation request received for one of these independent LUs has failed.

0021
An RNAA(Add) was received by the boundary function for a resource defined at system definition time, which is not allowed.

VTAM hint:

- A physical connection must exist for a resource if you are attempting to use dynamic reconfiguration. For more information about dynamic reconfiguration, see z/OS Communications Server: SNA Network Implementation Guide.
- This error can occur for a physical unit if a network address has been specified on the ADDR operand of the PU definition statement, but there is no physical connection for the resource. For more information about the ADDR operand, see z/OS Communications Server: SNA Resource Definition Reference.

0022
The link for which ACTLINK was issued is an S/390® channel path that has been defined for connections only to a Type 2.1 node. However, the SSCP that sent ACTLINK had previously indicated it does not support Type 2.1 connections.

0023
Modem test support cannot be changed. The RNAA or SETCV containing the SDLC secondary station (X'03') or the extended SDLC secondary station (X'43') control vector is rejected.

0024
The data mode cannot be changed. The RNAA or SETCV containing the SDLC secondary station (X'03') or the extended SDLC secondary station (X'43') control vector is rejected.

0025
The receiving node is unable to process a BIND for the LU type specified for the given LU name.

0026
A link is defined as not supporting HPR, but the port supports only HPR links.

VTAM hint: Possible reasons for this error include, but are not limited to, the following ones:

- A connection over a native ATM SVC cannot be established because the TG is not defined to support APPN and HPR.

  One or more values are coded incorrectly on a PU definition statement in a switched major node that defines an APPN TG over a native ATM SVC. These incorrect values might be on the HPR, CONNTYPE, or PUTYPE operands, which must specify HPR=YES, CONNTYPE=APPN, and PUTYPE=2 for native ATM connections. Any other values coded on these operands cause a connection over a native ATM SVC to fail.
- Dial-out or dial-in attempts to establish a session over an Enterprise Extender connection fail.

  The selected link station does not have HPR=RTP capability. To resolve this problem, specify one of the following start options:

  – Start option HPR=RTP
  – Start option HPR=(RTP,ANR). Specify HPR=YES either on the PU definition statement or on the operator command activating the PU.

0027
A link connection request for a non-empty active link connection configuration was received by the management services element; the active link connection configuration of the DLC element is empty; that is, it has no link connection components present.

0028
An RNAA(Move) was received for an adjacent link station (ALS), and the TO and FROM links were neither both primary nor both secondary.

0029
The RU refers to a resource, and the sender and receiver disagree about its status. One considers it a static resource, the other a dynamic resource.

002A
A session cannot be activated because the node does not support segment generation and the maximum link BTU size is too small to satisfy a requirement on the minimum send RU size as defined for the session mode.

002B
A session cannot be activated because the node does not support segment reassembly and the maximum link BTU size is too small to satisfy a requirement on the minimum receive RU size as defined for the session mode.

002C
BFSESSINFO was received reporting a subject LU in another network, or BFINIT was received with a NETID specified for the PLU which was not the same as the NETID of the ALS (XNETALS=YES) or the receiving SSCP (XNETALS=NO).

002D
BFSESSINFO was received for an (independent) subject LU, but the reported LU is considered by the receiver as a dependent LU.

002E
BFSESSINFO was received reporting a dynamic subject LU that the receiver considers to be located under a different adjacent link station (ALS) than that reported in the BFSESSINFO. The SSCP will attempt to correct this configuration mismatch.

002F
BFSESSINFO was received reporting a subject LU that the receiver considers to be located under a different adjacent link station (ALS) than that reported in the BFSESSINFO. The SSCP cannot correct this configuration mismatch.

0030
BFSESSINFO was received for a subject LU, but the receiver has the address associated with a different LU, which it considers to be static.

0031
BFSESSINFO was received for a subject LU, but the receiver has the address associated with anything other than a static LU or cross-domain resource.

0032
BFSESSINFO was received for an LU. The subject LU is verified, but, for a given session, either the partner LU is reported as the primary and the receiver does not consider that LU to be primary-capable, or the partner LU is reported as the secondary and the receiver does not consider that LU to be secondary-capable.

0033
Upon receipt of BFSESSINFO, the receiver considers the control block associated with a partner LU to be a cross-domain resource that is not active or an application that is not active.

0034
Upon receipt of BFSESSINFO, the receiver considers the control block associated with a partner LU to be neither an LU, cross-domain resource, nor an application.

0035
A network address was returned in RSP(RNAA) that the receiver believes is already associated with a different resource.

0036
BFSESSINFO was received containing an adjacent link station (ALS) address that was not valid. For example, the ALS does not represent a Type 2.1 node.

0037
BFSESSINFO was received for a subject LU, where the secondary address specified in the BFSESSINFO does not match the secondary address the SSCP believes is associated with the LU.

0038
The subject LU specified in the BFSESSINFO RU is not defined to the SSCP as an LU or a cross-domain resource.

0039
A request that is valid only for a switched subarea link was received for a link that is not subarea-capable.

003A
A request that is valid only for a nonswitched subarea link was received for a subarea dial link.

003B
An RNAA (add) was received for an LU; however an LU with the same name but a different local address already exists under the specified ALS.

0041
Takeover processing completed, but the SSCP did not receive a BFSESSINFO for a resource that the SSCP believed to be a static, independent LU.

0042
A BFINIT sent by the boundary was processed by the SSCP and the PLU resource is not owned by this SSCP. This is probably the result of a TAKEOVER and GIVEBACK occurring before the BFINIT was processed by the SSCP. This might also be caused by a definition error for the PLU.

0043
A request was received for a nonswitched resource that is valid only for a switched resource.

0044
X.21 dial and auto-call capability not present—resource mismatch.

0045
A session request was received and the NETID for the resource does not match that of the adjacent link station providing service for the resource.

VTAM hint: When a VTAM host has a Type 2.1 connection to a gateway NCP (XNETALS=YES is specified), a different VTAM host must own the Type 5 connection to the NCP.

0046
A CONNOUT was received indicating the sender and receiver have a system-definition mismatch: the CONNOUT connection type field specified a nonswitched link, but the receiver does not define the affected node as a T2.1 node on a nonswitched link or as one that supports XID3 exchange.

VTAM hint: This sense code can be displayed in a VTAM message but is set by another product. It might be issued by NCP. See *NCP V7R8, SSP V4R8, EP R14 Messages and Codes* for a description of sense codes set by NCP.

0047
A session request or BFSESSINFO request was received and the network ID for the OLU or the subject LU does not match that of the adjacent link station providing service for the resource.

0048
The DLU is an independent LU but the selected boundary function is not independent LU capable.

0049
A BFSESSINFO request was received but the subject resource is not active.

0050
The element address of an intra-FRSE PVC segment subport specified in a SETCV resides on the same frame-relay port as another subport within a subport set.

0051
The maximum frame size in the system — definition differs for any two partners in an intra-FRSE PVC segment subport set specified in a SETCV.

0052
Adjacent frame-relay equipment management protocols are not supported on either of the frame-relay ports for the primary or its backup subport specified in the SETCV for the intra-FRSE PVC segment subport set.

VTAM hint: A possible cause of this error is that there is a conflict in the coding of the PU definition and the FRSESET definition.

A backup PU has been coded in the FRSESET definition statement, but either this backup PU or its corresponding primary PU was coded on a line that has LMI=NO coded.

In order to have backup, the primary and backup PUs must be defined on lines whose link-station subport supports local management interface (LMI) protocol (LMI=ANSI or LMI=CCITT coded on the first PU definition statement under the LINE definition statement). For information about the LMI keyword, see *NCP, SSP, and EP Resource Definition Reference*.

0053
A node identifies itself as a extended border node for some sessions but claims not to be a extended border node for other sessions.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product.

0054
SETCV was received to define an intra-FRSE segment subport set between subports that are incompatible; one of the subports does not support alternate physical paths.

0055
SETCV was received to define an intra-FRSE segment subport set between subports that are incompatible; one of the subports is on an outboard DLC and the other is not on an outboard DLC.

0056
A CPSVRMGR session cannot be established over a LEN connection that is not of type TCP.

Sense code 0878

Insufficient storage: The storage resource required for a data format is not available.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
CONNOUT contained more dial digits than can be stored by the receiving product.

Sense code 0879

Storage medium error: A permanent error has occurred involving a storage medium.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Disk I/O error.

0002
I/O error: Load module and dump and re-IPL switches are not saved to disk.

0003
I/O error: Automatic dump switches are not saved to disk.

Sense code 087A

Format processing error: A processing error occurred during data formatting.

Sense code 087B

Resource unknown: The request contains a session key that does not identify a session known to some gateway node; for example, a session activation request arrives at a gateway node after it has released the address transform for the intended session.

Sense code 087C

SSCP-PU session not active: A gateway SSCP-PU session that is needed to establish an address transform for the intended cross-network LU-LU session was not active, or the gateway node is not defined.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

Bytes 2 and 3 contain sense-code-specific information that indicates the specific reason for not rerouting the request.

0000
No specific code applies.

VTAM hint: A possible cause of this error is that the SSCP-PU session is not active on the DLU side.

This sense code might not indicate an error. If the destination side cannot use the request network address assignment (RNAA) to obtain network addresses for communication across the network boundary, it will issue the 087C0000 sense code and the origin side will have to obtain the network addresses. So you might see this sense code but the session will set up successfully.

0001
An SSCP in the session setup path for an LU-LU session has lost connectivity with a gateway node traversed by the session, and has no other way to learn that the session has ended. An intermediate SSCP sends this sense data to one adjacent SSCP when it had previously lost connectivity with the other adjacent SSCP on the same session setup path. An endpoint SSCP sends this sense data to its adjacent SSCP when it had previously lost connectivity to a dependent LU or the boundary function of an independent LU.

0002
The SSCP lost connectivity with the boundary function of an independent PLU after the LU-LU session was started, and has no other way to learn that the session has ended; the SSCP either never had a session to a gateway node in the LU-LU session path, or had previously lost connectivity to it.

0003
The SSCP lost connectivity with the boundary function of an independent SLU after the LU-LU session was started, and has no other way to learn that the session has ended; the SSCP either never had a session to a gateway node in the LU-LU session path, or had previously lost connectivity to it.

Sense code 087D

Session services path error: A session-services request cannot be rerouted along a path of SSCP-SSCP sessions. This capability is required, for example, to set up a cross-network LU-LU session.

Bytes 2 and 3 contain sense-code-specific information that indicates the specific reason for not rerouting the request.

0000
No specific code applies.

VTAM hint: A possible cause of this sense code is an error in the CDRM definition.

0001
An SSCP has attempted unsuccessfully to reroute a session services request to its destination via one or more adjacent SSCPs; this value is sent by a gateway SSCP or a nongateway SSCP when it has exhausted trial-and-error rerouting.

Note: This code is used when SSCP rerouting fails completely. The remaining codes are used for failures to reroute to a particular SSCP. For example, they are associated with specific SSCPs when information about a rerouting failure is displayed in the node that was trying to reroute.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- VTAM knows which node owns the LU but is not able to route a directed search to that node to verify the availability of the LU. If messages IST894I and IST895I are issued and indicate that one of the adjacent SSCPs was ISTAPNCP with a failure sense of 087F0001, this is probably the reason for the error.

  Verify that a valid search path exists. This can be CP-CP sessions and/or a subarea path. One possible cause of the problem is the absence of a CP-CP session between two nodes that share an active CP-CP capable link. If this is the case, take one of the following actions:

  – Reactivate the CP-CP session.
  – Deactivate the link and reactivate it as a link that is not CP-CP capable so that topology and routing services will know that it is no longer available for use in directed search routing.
- There is no SSCP-SSCP session.
- The half-session control block (HSCB) count is too low in the NCP to handle the number of sessions. A possible solution to this problem is to code a larger value on the ADDSESS keyword of the BUILD definition statement and regen.
- Both sides are using the same SSCP name.

0002
An SSCP is unable to reroute a session services request because a necessary routing table is not available. This means that there is no adjacent SSCP table corresponding to the rerouting key in the resource identifier control vector. The receiver of this value will, if possible, try rerouting to another SSCP.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0003
This sense code is set in either of these two cases:

- A CDINIT is received from an ADJSSCP (OLU), and the CDRM statement for the ADJSSCP (OLU) does not allow this SSCP to build a dynamic CDRSC (CDRSC=REQ).
- An SSCP (OLU) or SSCP (INT) built a dynamic CDRSC for the DLU, but the ADJSSCP (DLU) selected does not allow this SSCP to build a dynamic CDRSC.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0004
Session services path error: Conflict in gateway capabilities support.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0005
An SSCP is unable to use the gateway node specified in CDINIT because that gateway node cannot allocate an address transform for the intended cross-network LU-LU session.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0006
An SSCP is able to use only a subset of the alternate gateway nodes available to it. However, for the subset that it can use, none can provide the needed alias address pair.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0007
An SSCP is unable to reroute a session services request. One of the session partners was defined as a real CDRSC, as well as a CDRSC without netid. This is not allowed.

0008
The adjacent SSCP does not support the requested CDINIT function (for example, notification of resource availability or XRF).

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0009
Network address not valid: NCP returned an address that was already in use for a different session. The initiate request cannot be rerouted.

000A
An SSCP is unable to reroute a session services request because the request has been routed through the same SSCP twice.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: This error can occur during an attempt to take over a switched connection because a connection-network-capable control point (CP) on the connection network does not have a complete system definition. See the information about common APPN problems in z/OS Communications

Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this session takeover problem.

000B
The DLU specified in the CDINIT is unknown to the receiving SSCP, and the receiving SSCP cannot reroute the CDINIT.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

000D
An SSCP has purged a session services request because the adjacent SSCP did not respond to the request within a specified installation-defined time limit.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM Hint: A possible cause of this error is that the response from the CDINIT sent toward the DLU has not been received during the operator specified time interval. The CDINIT timed out, and a negative CDINIT response is assumed.

000E
A locate search request was limited because a prior search had determined that the subject target resource was not currently accessible and the search delay thresholds had not yet been met.

VTAM hint: The resource was not found. A locate search request was limited because a prior search had determined that the subject target resource was not currently reachable (a valid search reduction entry exists).

Sense code 087E

SSCP visit count exceeds limit: The SSCP visit count specified in the session services request—CDINIT, INIT_OTHER_CD, or DSRLST—has been decremented to zero. The session services request has been routed through an excessive number of SSCPs. (The SSCPs are not necessarily distinct.)

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

Sense code 087F

Session services path error: A session services request cannot be rerouted into an APPN-subarea network.

Bytes 2 and 3 contain sense-code-specific information that indicates the specific reason for not rerouting the request.

0000
No specific code applies.

0001
A Locate/CD-Initiate reply, indicating resubmit on directed search, was received after a directed search had been performed in response to a previous Locate/CD-Initiate reply.

0002
A search request was received that was duplicated or not valid.

0003
A subarea search was not routed into an APPN network because a requested function was not supported by the APPN-subarea interchange node.

0004
An APPN search was not routed into a subarea network because a "search of subarea" was not permitted.

0005
A subarea search was not routed into an APPN network because the request originated in the APPN network containing this node and the APPN network is capable of executing a broadcast search.

0006
Subarea search not routed into APPN network because a required component was not available.

0007
This sense data value is generated when an interchange node receives a Locate/CD-Initiate request from an APPN network that contains a control vector X'5D' (subfield X'81') and does not route to SSCPs in the network specified in that control vector because its disjoint network indicator is not set.

0008
An APPN search (or a search on behalf of a DLUS-served resource) was not routed to a subarea SSCP that will be or has already been searched using the APPN network.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0009
An APPN locate search request with an alias network ID was rejected by a border node that does not support ALIAS searches.

000A
An APPN locate search request that contains a network qualified target LU name was rejected by a border node because the border node does not allow searches for the specified target network ID.

Sense code 0881

ACTCDRM failure—REQACTCDRM sent: An SSCP-SSCP session-activation request, ACTCDRM, cannot be rerouted to a gateway SSCP because, at some gateway PU, the necessary transform is not complete and the gateway PU has sent REQACTCDRM to the gateway SSCP.

Sense code 0884

ACTCDRM failure—no REQACTCDRM sent: An SSCP-SSCP session activation request, ACTCDRM, cannot be rerouted to the destination SSCP because, at some gateway node PU, the necessary transform is not complete and REQACTCDRM cannot be sent to the destination SSCP because the gateway SSCP-PU session is not active or the intended SSCP session partner does not provide gateway services.

Sense code 0885

Same-Network routing not supported: The requested function cannot be executed, because the SSCP will not reroute a request within its subnetwork. A CDINIT request has been received across a dynamic subarea interconnect gateway route from another node in this subnetwork or across a gateway node; or a CDINIT request has been received from another node in this subnetwork or through a gateway node that needs to be rerouted to another node in this subnetwork across a dynamic subarea interconnect gateway route. This error most likely results from a network configuration problem in which a node has been defined to have dynamic subarea interconnect gateway VRs and nondynamic subarea interconnect gateway VRs within the same subnetwork.

Sense code 0886

Subnetwork rerouting not supported: An SSCP received a session services request—CDINIT, INIT_OTHER_CD, NOTIFY (vector key=X'01'), or DSRLST—from an SSCP in its subnetwork that, if rerouted, would not cross a subnetwork boundary. The SSCP does not support rerouting within a subnetwork.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

Sense code 0887

Dequeue retry unsuccessful—session remains queued: The SSCP cannot successfully honor a CDINIT(Dequeue) request. The request specifies "leave on queue if dequeue-retry is unsuccessful." The SSCP has left the queued session on its queue.

Sense code 0888

Name conflict: A name specified in an RU is unknown, or is known and does not have the required capabilities, or is a duplicate resource for the specified resource type. When a name conflict is detected, further name checking ceases; multiple name conflicts are not reported or detected.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

VTAM hint: Sense code 0888000*n* might be issued when an attempt to establish a session fails in an intermediate VTAM along the session setup path. This error might occur because the intermediate VTAM that set the sense code is operating with NQNMODE=NAME or is a pre-V4 VTAM. Therefore, the intermediate VTAM cannot define multiple resources with the same name even though the network identifiers are different.

Change the intermediate domain to operate with NQNMODE=NQNAME to allow definition of multiple resources with the same name and different network identifiers, or reroute the session through another path.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0001
The specified DLU real network name is known, but identifies a resource that is not LU-LU session capable.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: A possible cause of this error is a duplicate resource in the same network.

0002
The specified DLU alias network name is known, but identifies a resource that is not LU-LU session capable.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0003
The specified OLU real network name is known, but identifies a resource that is not LU-LU session capable.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0004
The specified OLU alias network name is known, but identifies a resource that is not LU-LU session capable.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0005
Name translation was not valid; that is, a different LU name was returned with the same network ID as the original LU name.

0006
The specified DLU real network name is known, but is a duplicate resource.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- The same resource has been defined in the network in more than one location.
- If the origin LU is in APPN, this sense code can be issued if the destination resource has moved and the new location is not known throughout the network. This situation will be corrected when the origin LU receives this sense code and discards the incorrect information.
- If a LEN connection is being used, a possible cause of this error is that the network ID predefined for the cross-domain resource is the same as the network of the LEN connection but is not the same as the network where the resource resides. To fix this, move the CDRSC definition statement for the resource before any NETWORK definition statements so that the resource does not have a predefined network ID.

0007
The specified DLU alias network name is known, but is a duplicate resource.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: A possible cause of this error is that VTAM is unable to determine the DLU real name for a TR_REPLY RU. Ensure that the network ID is correct. To determine where the error occurred, look in the alias translation table for the alias name and the real name associated with it. Find the name that was given as the DLU alias name in IST664I and try to determine what the actual resource is in this host.

See z/OS Communications Server: SNA Network Implementation Guide for a description of alternatives to predefining cross-network destination logical units.

0008
The specified OLU real network name is known, but is a duplicate resource.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0009
The specified OLU alias network name is known, but is a duplicate resource.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

000A
A predefined real resource name and a predefined alias resource name were found for the same resource.

000B
A cross-network DLU name is defined as a shadow resource, but shadow resources are not supported for cross-network sessions.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

000C
A cross-domain or cross-network DLU name matches an alternate application name. However, the alternate application name is not the real name of the resource. This is only allowable in a same-domain session.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

000D
When processing a session initiation RU, an SSCP has found two different resource definitions for the OLU, one with the real OLU name and one with the alias OLU name.

000E
When processing a session initiation RU, an SSCP has found two different resource definitions for the DLU, one with the real DLU name and one with the alias DLU name.

000F
The specified DLU network name is defined as a generic resource. The session should be reinitiated using the name of an LU.

VTAM hint: This sense code is issued in connection with generic resources and the centralized definition of cross-domain resources function.

For an overview of centralized definition of cross-domain resources and information about how to set up these definitions, see z/OS Communications Server: SNA Network Implementation Guide.

0010
The LU 6.2 partner returned a name in the User Data field of its RSP(BIND) that differs from the name it returned in the User Data field of its RSP(BIND) for a previous BIND. Either the partner changed its name or name changes in the network have caused delivery of the latest BIND to a different partner.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- The partner LU might have changed names or name changes in the network have caused delivery of the latest BIND to a different partner LU.
- Name manipulations in the network are inconsistent or the network is finding different targets for the same name on subsequent BINDS.
- A partner LU incorrectly using the sender's name might have caused a problem.

0011
The LU 6.2 partner receiving a BIND carrying one specific target SLU name returned a name in the User Data field of its RSP(BIND) that is the same as it returned in response to a previous BIND carrying a different target SLU name.

VTAM Information: The partner LU name returned in the user data field of the BIND response was found in a VARIANT_NAME entry, but the SUPPLIED_ NAME entry used when the session was initiated indicates (by the associated name field) that no name associated has taken place. The name returned in the user data field of a BIND response found in a SUPPLIED_NAME LU entry is different from the SUPPLIED_NAME entry used in the setup of the session.

VTAM hint: A possible cause of this error is that the name returned is identical to a name currently in an internal table as a name that has already been supplied by the application.

0012
A session initiation request is received from the partner LU containing a LUNAME found in an internal table, but with a different network qualifier.

VTAM Information: Name changes in the network have caused alteration of the network identifier.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- The local LU does not support network-qualified names.
- A non-flat name space was detected where a flat name space is required.

0013
A border node received a topology database update (TDU) from a node within its local subnet containing the CP name of a node that is adjacent to the border node across an intersubnet TG.

0014
An excessive number of topology database updates (TDUs) have been processed for a resource.

0015
A generic name of a resource has been received when only the real name of the resource can be specified.

0016
The DLUR-specified network name is known, but is a duplicate resource.

Sense code 0889

Transaction program error: The transaction program has detected an error.

This sense code is sent only in an FMH-7.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
Program error—no data truncation: The transaction program *sending* data detected an error but did not truncate a logical record.

Program error—purging: The transaction program *receiving* data detected an error. All remaining information, if any, that the receiving program had not yet received, and that the sending program had sent prior to being notified of the error, is discarded.

0001
Program error—data truncation: The transaction program *sending* data detected an error and truncated the logical record it was sending.

0100
Service transaction program error—no data truncation: The service transaction program *sending* data detected an error and did not truncate a logical record.

Service transaction program error—purging: The service transaction program *receiving* data detected an error. All remaining information, if any, that the receiving service transaction program had not yet received, and that the sending service transaction program had sent prior to being notified of the error, is discarded.

0101
Service transaction program error—data truncation: The service transaction program *sending* data detected an error and truncated the logical record it was sending.

Sense code 088A

Resource unavailable—NOTIFY forthcoming: The SSCP cannot satisfy the request because a required resource is temporarily unavailable. When the required resource becomes available, the NOTIFY NS keys X'07' or X'08' will be sent.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
SSCP-SSCP session not active: A SSCP-SSCP session required to reroute the cross-network request was not active.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0003
SSCP-LU session not active: The SSCP(DLU) is currently not in session with the DLU.

0004
LU session limit exceeded: The DLU is currently at its session limit and the requested session would cause the limit to be exceeded.

Sense code 088B

BB not accepted—BIS reply requested: Sent in response to a BB (either an LUSTAT bid or an Attach) to indicate that the receiver has sent a BIS request and wishes to terminate the session without processing any more conversations, but without sending an UNBIND. A BIS reply is requested so that the negative response sender can send a normal UNBIND. This sense code is sent only by LUs not supporting change-number-of-session protocols.

Sense code 088C

Missing control vector: The RU or XID did not contain a required control vector or subfield.

Bytes 2 and 3 following the sense code contain sense code-specific information.

***nn*yy**
Byte 2 contains the key (*nn*) of the subject control vector and Byte 3 (*yy*) contains the control vector's type or the missing subfield.

0E00
The route setup request did not contain required control vector X'0E'.

0EF3
The name of the new PLU is missing from a third party initiated flow.

0EF4
A SLUINIT BIND was missing the PLU CP_NAME control vector X'0E'.

2600
The route setup request did not contain required control vector X'26'.

2B00
RSCV control vector X'2B' for an APPN session was not provided, or the route setup request did not contain required control vector X'2B'.

2C00
The route setup request did not contain required control vector X'2C'.

2D00
The route setup request did not contain required control vector X'2D'.

3100
BIND image control vector X'31' missing.

3900
NCE instance ID control vector X'39' missing.

4680
Missing subvector X'80' on TG descriptor X'46'.

4581
Missing directory extensions subvector control vector X'4581'.

4683
Missing subvector X'83' on TG descriptor X'46'.

4700
TG characteristics control vector X'47' missing following a TG descriptor control vector X'46''.

5F00
Control vector X'5F' missing.

6000
Control vector X'60' missing.

6380
Control vector X'63' crypto capabilities (control vector X'80') missing.

6500
Device characteristics control vector X'65' missing.

6700
The route setup request did not contain required control vector X'67'.

8000
Control vector X'80' missing.

8100
Control vector X'81' missing.

Sense code 088D

Duplicate network name: An SSCP has detected a violation of the requirement that network names used across multiple domains be unique within the multiple-domain network. For example, the SSCP(DLU) has detected that the OLU name received in CDINIT is currently also defined in the domain of the SSCP(DLU).

Sense code 088E

Capability mismatch: A network component detected a capability mismatch between different resources involved in the same network function. For example, an SSCP detects that an LU has been assigned a subarea address too large for one of the other resources involved in the session initiation to support.

Bytes 2 and 3 following the sense code contains sense-code-specific information.

0000
A resource encountered during LU-LU session initiation is not ENA-capable; the session initiation request might be rerouted.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0001
A resource encountered during LU-LU session initiation is not ENA-capable; the session initiation request should not be rerouted.

0002
An SSCP has requested a "pre-ENA compatible" SLU address for an SLU that already has an ENA address.

0003
The gateway node selected by the gateway SSCP from the gateway node list is not ENA-capable when an ENA-capable gateway node is required. Another gateway node might be tried.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0004
During a dynamic path update, the SSCP detected that the update contained a path with an explicit route (ER) number greater than seven and the target node did not have extended subarea addressing capabilities. Therefore, the dynamic path update information for this destination subarea is not being sent to the target node.

0005
The session could not be established because a specified extended subarea address exceeded that allowed at a node along the selected session setup path. The gateway SSCP doing gateway node selection might try the session setup again by selecting another gateway node having a larger subarea address limit in the network containing the DLU.

VTAM hint: This sense code is issued when there are incompatible ESA capabilities along the session setup path. The DLU direction subarea address is greater than the OLU direction capabilities.

0006
The session could not be established because a specified extended subarea address exceeded that allowed at a node along the selected session setup path. The gateway SSCP doing gateway node selection may try the session setup again by selecting another gateway node that uses a smaller subarea address in the network containing the DLU.

VTAM hint: This sense code is issued when there are incompatible ESA capabilities along the session setup path. The OLU direction subarea address is greater than the DLU direction capabilities.

0007
During a dynamic path update, the SSCP detected that the update contained a path definition with a subarea address above 255 and that the target node did not support extended subarea addressing. Therefore, the dynamic path update information for this destination subarea is not being sent to the target node.

0008
The session could not be established because the dependent LU server detected an incompatibility between its capabilities and those of its dependent LU requester.

0009
The session could not be established because the dependent LU requester detected an incompatibility between its capabilities and those of its dependent LU server.

000A
An attempt was made to establish a connection between a boundary function that does not support cross-subnetwork connections and a border node.

000B
The extended border node indicator was set during XID exchange but both the border node and intersubnetwork extended session services support indicators were not set in the CP capabilities GDS variable.

000C
There is an APPN subnetwork link mismatch. Two nodes might have a system definition mismatch or two nodes might already have a non-APPN subnetwork connection active and one attempts to activate an APPN subnetwork connection.

VTAM hint: An attempt was made to activate two or more links between two nodes in which at least one of the links is defined as an APPN intersubnetwork link, but not all the links are defined as APPN intersubnetwork links. Determine what type of links should be defined between the two nodes in your network. Then modify the NATIVE option on the PU definition to reflect this.

000E
Virtual-route-based transmission group does not support nonnative connections.

VTAM Information: VTAM sets this sense code when a virtual-route-based transmission group connection is requested between two adjacent nodes connected by a nonnative, Type 2.1 connection. The request for the VRTG connection will fail. The SSCP-SSCP session will also fail.

000F
An attempt was made to establish a CP-SVR pipe across a subnetwork boundary between a dependent LU server and a dependent LU requester with limited multi-subnetwork support.

Sense code 088F

XRF procedure error: A request was received for an XRF-active or XRF-backup session and was not acted on.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0003
A SWITCH request specifying a switch to the already existing state was received.

0004
A SWITCH request was received that was not valid.

0005
The SLU has received SWITCH (Conditional, to backup) and no current XRF-backup sessions exist that can replace this session (that is, become the XRF-active session).

0006
An INITIATE request for an XRF-backup session was received that allowed queuing. (XRF-backup and session queuing are mutually exclusive functions.)

0007
An initiation request for an XRF-backup session was received specifying an XRF-backup session, and the DLU does not support XRF sessions.

0008
An XRF-active BIND was received with a session correlation identifier that duplicates a session correlation identifier associated with an existing XRF session.

0009
An XRF-backup BIND was received for an LU that currently does not have an XRF session.

000A
Cryptography not supported: An XRF BIND was received indicating cryptography. A cryptography key must be defined for the NCP session as well.

000B
An initiation request for an XRF-backup session was received specifying an XRF-backup session, and the OLU does not support XRF sessions.

000F
Backup command not valid.

0010
An XRF-backup BIND was received with a session correlation identifier that does not match the session correlation identifier associated with the existing XRF session with that LU.

0011
Cryptography information could not be obtained for the backup XRF session.

0012
An XRF-backup BIND associated with the existing XRF session supporting data compression was received that did not support compression.

0013
The existing session was negotiated using an extended BIND carrying the length-checked compression (X'66') control vector, but the XRF-backup BIND is nonextended.

0014
The message authentication code level of the extended recovery facility (XRF) backup session does not match that of the XRF primary session.

0015
The NCP level did not support the MAC level with XRF.

Sense code 0890

Search failure.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0010
Routing error during a directed search: A Locate GDS variable for a directed search was received by an intermediate NNCP and could not be successfully routed to the destination control point.

0011
The path used to transport the directed Locate request (a message containing Locate, Find Resource, and Cross-Domain Initiate GDS variables) does not support a sufficiently-large Locate message size to return the Locate response (a message containing Locate, Found Resource, and Cross-Domain Initiate GDS variables). The NNS(OLU) was requested to try the directed search again over a path supporting a sufficient Locate message size.

0020
Resource not found during a directed search: A Locate GDS variable for a directed search was received by the named destination CP and the search argument resource is not a local resource.

0021
Verification reduction could not be satisfied, but was required for the request. This sense code is returned when resource verification reduction cannot be satisfied for the DLU.

VTAM hint: This sense code is set by the PLU's network node server when resource verification reduction could not be satisfied for a request initiated by the PLU control point to obtain the RSCV from the network node server.

0022
Destination of search not served by this CP.

0028
Resource not found, broadcast required: The resource was not found on a directed LOCATE/CDINIT search, and a restricted broadcast was executed at the destination and failed; a broadcast should be tried.

0030
Resource deleted, no broadcast required: A Locate GDS variable for a directed search was received by the named destination CP and the search argument resource has been deleted.

0036
Duplicate search to a subnetwork. This is an attempt to search a network previously reached by this search procedure. This condition indicates an attempt to loop back into a subnetwork through a different entry point.

0037
Unknown TG vectors to dependent LU requester. A resubmitted Located search for a dependent LU at its dependent LU requester was unsuccessful. This condition arises only after the dependent LU server has verified the existence of the dependent LU.

VTAM hint: VTAM was unable to successfully locate the dependent LU requester (DLUR) node in order to obtain the necessary DLUR endpoint transmission group (TG) vectors. The current session setup will fail. Verify that connectivity exists between the node that issued the sense code and the DLUR node.

0038
Too many directed search subprocedures: A LOCATE exceeded the maximum height of the search tree; too many directed search subprocedures were tried; no retry.

0040
Resource not found during a broadcast search: A Locate GDS variable for a broadcast search was received by a CP that does not provide network services for the search argument resource and neither do any of the CPs searched in its broadcast subtree. This condition is detected by crossing search requests (a CP sends and receives a search request with the same PCID and the same search argument resource) or by a local search failure and all CPs in the broadcast subtree returning this sense data.

0048
Neutral reply received from an end node: A locate reply with no found and no extended sense data (X'35') control vector was received from an APPN end node.

0050
Quiesced CP: A CP in the broadcast search tree is in a quiescent state and, therefore, not receiving Locate GDS variables. This condition is detected when a CP in the search subtree is quiesced and no other CP in the subtree found the requested resource.

0060
Storage not available: A CP in the broadcast search tree does not have sufficient storage to participate in the search and no other CP in the search subtree found the requested resource.

0070
Session outage: A CP in the search tree has lost its CP-CP session with a CP that had been sent a Locate GDS variable and no reply had been received.

0080
Duplicate fully qualified PCID: A CP in the search tree detected a duplicate fully qualified PCID for a different session request from the session request that first used the fully qualified PCID.

0081
PCID modifier too long: A PCID modifier list was received that had a length greater than ten bytes.

0082
PCID modifier space exhausted: A PCID modifier list was received that contained the maximum of ten bytes. As the maximum list size has been reached, another list entry cannot be made that was longer than ten bytes.

VTAM hint:

This sense code is issued when a node determines that it might have to retry, resubmit, or redirect a search, but it cannot allocate a procedure-correlation identifier (PCID) Modifier slot, because all 20 half-byte slots have already been allocated. This indicates that the search has been exhausted (20 nodes have already allocated slots without finding the DLU). There is currently no recovery action architected or implemented to recover from this situation.

The PCID Modifier slots differ from the SSCP visit count in that the SSCP visit count is decremented by every SSCP on the session setup path. The PCID Modifier slots are not allocated by every SSCP, only those that might have to perform retried, resubmitted, or redirected searches.

Sense code 0891

Network ID (NETID) not valid.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
PLU NETID not valid: The NETID of the PLU is not the same as that of the SSCP(PLU).

0002
NETID not valid: The NETID field in CONNOUT does not match the NETID defined in the link station receiving the CONNOUT.

0003
NETID not valid: The NETID field in the RNAA is not the same as the native NETID. There is a mismatch between the system definitions of the SSCP and the Type 4 node.

0004
The network name control vector appended to the received XID3 does not contain a valid network ID. The network ID, preceding the CP name, must be greater than zero and less than eight bytes in length.

Alternatively, a network ID was received as an entry in a register GDS variable without an accompanying resource name, resulting in a resource name at the receiver that is not valid; the entry was not registered.

0005
The network name control vector appended to the received XID3 does not contain a valid CP name. The CP name, following the network ID, must be greater than zero and less than eight bytes in length.

0006
Invalid NETID: The sender has deactivated CP-CP sessions with the adjacent nonnative CP because one of the following situations has occurred:

- Neither CP contains border node support (that is, neither sets Byte 9, Bit 7 to one in the CP capabilities GDS variable that it sends).
- One or both nodes defined the connection as native, which is not allowed if the network IDs are different.

VTAM hint: If this sense code is displayed in message IST1280I, this probably indicates that CP-CP sessions were attempted between two network nodes in different networks. If a nonnative relationship is desired, ensure that BN=YES is coded to enable border node support. Also ensure that NATIVE=YES is not coded on a PU or ADJCP statement representing the partner node.

If a native relationship is desired, modify the VTAM start lists for the specific nodes so that both start lists specify the same network.

0007
NETID not valid: Establishment of a switched link connection failed because the NETID of the destination PU was not equal to that of the requesting SSCP.

0008
Insufficient control blocks for dynamic network ID assignment. A CONNOUT specified a network ID that is not currently defined and sufficient control blocks are not available.

0009
The network ID specified in the VRID list (X'1B') control vector is not valid.

000A
Network ID not valid: the network ID in the network name control vector does not match the network ID of the target resource of the REQACTPU.

Sense code 0892

Automatic network shutdown (ANS) has occurred.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Session reset when ANS=STOP: The SSCP controlling the LU has been lost. The session will be terminated because ANS=STOP was specified for this LU.

0002
The session was in pending-active state when the SSCP failed. However, because ANS=CONT, LU-LU sessions would normally continue, but because the session was not completely set up, it was reset.

0003
XRF-backup session reset when ANS=STOP: The XRF-backup session was reset because ANS=STOP was specified.

Sense code 0893

Takeover not complete.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
PLU lacking a control point, retry: The PLU is not currently receiving network services from a control point. The BIND is rejected because the session cannot be established. This sense data is returned by the boundary function of the PLU.

0002
SLU lacking a control point, retry: The SLU is not currently receiving network services from a control point. The BIND is rejected because the session cannot be established. This sense data is returned by the boundary function of the SLU.

0003
Sequence error: The SSCP should not send an RNAA for an independent LU until the takeover sequence is complete for the link station, that is, until all BFSESSINFOs for that LU have been received and accepted.

Sense code 0894

Migration support error: The sender of the request is relying on migration support that is not available.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
BIND cannot be extended: A BIND that is not an LU 6.2 BIND was received and cannot be extended by the receiver.

Sense code 0895

Control vector error: The RU or XID contained a control vector that was in error. Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

xxyy
Byte 2 (xx) contains the key of the control vector first detected in error. If more than one control vector is in error, only the first erroneous one is reported. Byte 3 (yy) of the sense code specific data contains the (zero-origin) byte offset of the error within the control vector.

Sense code 0896

Control vector too long.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Network name (X'0E') control vector is too long; the vector data portion is greater than 18 bytes long.

Sense code 0897

System definition mismatch: The requested function is not supported by the receiver, or there is a mismatch between the sending and receiving system definitions.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The BFCLEANUP specifies that it is for an independent LU, but the LU specified is not an independent LU. This also could be caused by a resource mismatch.

0002
The target LU is not in the same subarea as the Type 4 node.

0003
The function is not supported by the target resource.

0004
SLU name not valid: The network ID (if present) for the NS SLU name field is not equal to the network ID of the Type 4 node, or the SLU name is not equal to the LU name field in the LUB.

0005
The LU address specified in the FNA is not associated with the PU target address specified in the FNA.

0006
The SSCP has no predefinition for an LU and does not support dynamic resource definition.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0007
The receiving SSCP has a different system-defined name for the SSCP(DLU) than the SSCP(DLU) name in the session initiation request.

VTAM hint: In subarea, a possible cause of this error is that the CDRM definition statement in the OLU host for the DLU does not match what the DLU has coded for SSCPNAME in the VTAM start options.

0008
In a gateway with three gateway SSCPs, a gateway SSCP on the OLU side of the gateway was specified as having predesignated control in the CDINIT. In this configuration, only the middle gateway SSCP may have predesignated control.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0009
In a gateway with multiple gateway SSCPs, the gateway node assumes that one gateway is coded with GWCTL=ONLY. As a result, the gateway node receives gateway-control RUs from a different SSCP than the one it expects.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: A possible cause of this error is that the GWPATH definition specifies the wrong NCP name.

000A
The PU of an independent PLU named in BFINIT does not have the same element address as the one in the ALS field of BFINIT.

000B
An SSCP has detected a specification of gateway responsibility in the CDINIT request that is not consistent with its own definition. For example, an SSCP that has predesignated responsibility to control a gateway node specified in the CDINIT request sends this sense data when it receives the CDINIT from a session partner and the CDINIT indicates that the session partner also has predesignated responsibility for the gateway node; in this situation, a mismatch exists in the responsibilities of the SSCPs, because both cannot simultaneously have predesignated responsibility for the gateway node.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

000C
The receiver is unable to interpret the DLU name.

000D
Resource type not defined in receiver.

000F
A gateway node has received route data for a cross-network session in a form that it does not support.

0010
An adjacent SSCP has the same SSCP name as the SSCP that owns the DLU but a different network identifier than the DLU.

0011
The subsystem LU received CINIT with an appended LU definition (X'2F') control vector, but cannot process that control vector.

0012
The receiving SSCP has a different system-defined name for the SSCP(OLU) than the SSCP(OLU) name in the session initiation request.

0013
The session request (CDINIT) has routed back to the SSCP(OLU) or an SSCP on the session setup path has the same name as the SSCP(OLU).

0014
The MOSS automatic IPL/dump switches are not set properly.

0015
The OLU is represented using a dynamically defined resource but the ALS selected to provide its services does not permit dynamic definitions. The condition is detected when a session initiation request is received for an independent LU and no predefinition is found for the OLU resource. The session initiation is rejected.

VTAM hint: This sense code can be received when an unintended DYNLU value has been assigned to the PU that represents a link to an adjacent node. Only one DYNLU value can be associated with an adjacent node; the source of that value can be confusing. The DYNLU value is associated with an adjacent node when the first link to that adjacent node is activated. When the DYNLU value is associated with the adjacent node, that value is propagated to all links to that adjacent node when those links are activated. To determine the source of the DYNLU value for an adjacent node, search the message log prior to the receipt of this sense code for the unsolicited message IST2180I that contains the CP name of the adjacent node. See message IST2180I in z/OS Communications Server: SNA Messages for an explanation of this message. See the DYNLU combinations table in z/OS Communications Server: SNA Resource Definition Reference for more information about determining the source of the DYNLU value assigned to an adjacent CP and attached resources.

0016
The DLU is represented using a dynamically defined resource but the ALS selected to provide its services does not permit dynamic definitions. The condition is detected when a session initiation request is being processed for an independent destination LU and no predefinition is found for the DLU resource. The session initiation request is rejected.

VTAM hint: This sense code can be received when an unintended DYNLU value has been assigned to the PU that represents a link to an adjacent node. Only one DYNLU value can be associated with an adjacent node; the source of that value can be confusing. The DYNLU value is associated with an adjacent node when the first link to that adjacent node is activated. When the DYNLU value is associated with the adjacent node, that value is propagated to all links to that adjacent node when those links are activated. To determine the source of the DYNLU value for an adjacent node, search the message log prior to the receipt of this sense code for the unsolicited message IST2180I that contains the CP name of the adjacent node. See message IST2180I in z/OS Communications Server: SNA Messages for an explanation of this message. See the DYNLU combinations table in z/OS Communications Server: SNA Resource Definition Reference for more information about determining the source of the DYNLU value assigned to an adjacent CP and attached resources.

0017
The request was received for an independent LU over a specific ALS but that ALS is not defined to provide services for the subject LU. The condition is detected when a session initiation request is received and the ALS for which the request was received was not predefined to provide service for that independent LU. The session initiation request is rejected.

0018
Session Initiation Status Not Supported: A session initiation request was received that contained a session initiation status field that was not valid for the receiving node.

0019
The SSCP has received a CONTACTED or REQCONT containing an XID3 carrying an unrecognized CP name; the SSCP supports only predefined CP names.

001A
The source or destination service access point address (SSAP or DSAP) in the logical link control protocol data unit of the XID information field for a token-ring LAN is unknown.

Sense code 0898

Session reset: The XRF session is being reset.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The XRF-active session has been reset because the XRF-backup PLU forced a takeover.

0002
XRF-backup hierarchical reset: The identified XRF-backup LU-LU session is being deactivated because the related XRF-active session terminated normally. The LU sending this sense data is resetting its half-session before receiving the response from the partner LU. (See UNBIND Type X'12'.)

0003
XRF-active hierarchical reset: The identified XRF-active LU-LU session is being deactivated because the related XRF-backup session performed a forced takeover of this session (via SWITCH). The LU sending this sense data is resetting its half-session before receiving the response from the partner LU. (See UNBIND Type X'13'.)

Sense code 0899

Address not valid: An address modifying a control function is not valid, or outside the range allowed by the receiver.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0002
If the address requested in the RNAA is an existing address and an FNA has been received for this address, reject the RNAA.

0003
For a dynamic reconfiguration MOVE or REPLACE operation, the new LU local address specified in the RNAA is incompatible with the LU local address already specified in the control block. Both must be either zero or nonzero.

Sense code 089A

File not valid or file not found: The requested file was not found, or was not valid.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Requested file not found.

0002
Duplicate load module—one with same name already on disk. The load module cannot be added.

0003
Unable to locate required associated object.

0004
Another load module on the MOSS disk has the same IPL time as the one specified for the load module in the MODIFY LOAD command.

Sense code 089B

Session correlation exception: The session correlation procedure detected an exceptional condition at the SLU.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
RUs out of order: A BIND request with the correlating fully qualified PCID control vector (X'5F') arrived before UNBIND (Type X'02') was received for the correlated session. This sense data is sent in an UNBIND that terminates the correlated session.

0002
Correlator not found: A BIND request with the correlating fully-qualified control vector (X'5F') cannot be correlated to any previous session.

Sense code 089C

Duplicate session related identifier, URC not valid.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The URC received in the BFINIT duplicates a URC for an outstanding session initiation attempt from the same BF.

Sense code 089D

Gateway node error detected during cross-network session initiation.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0001
The gateway node list used to select a gateway node to cross a network boundary is exhausted. This error can be caused by an element address mismatch.

VTAM hint: A possible cause of this error is an element address mismatch between VTAM and NCP.

0003
RNAA has failed; another gateway node should be tried.

0004
Address conversion based on the subarea or element address split was unsuccessful.

0005
The gateway node selected by one gateway SSCP is not known to another gateway SSCP in the same gateway. This can be a system definition error in the gateway SSCP that does not recognize the gateway node.

0006
A gateway SSCP has found that a gateway node has assigned duplicate addresses.

Sense code 089E

Identified data object already exists.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0001
A request to create a new data object has failed because the identified data-object already exists at the target node.

0002
A request to replace a data object has failed because it specifies a to-be-deleted data object different from the to-be-stored data object; however, the to-be-stored data object already exists.

Sense code 089F

The node component required to satisfy a request is not currently available.

Bytes 2 and 3 following the sense code contain sense code-specific information.

0004
A session initiation has failed because a generic resource coupling facility is not available to do the necessary information update.

VTAM hint: This sense code is issued when VTAM is unable to access or create information about a generic resource in the MVS coupling facility structure for one of the following reasons:

- The coupling facility structure storage is exhausted. This might be a temporary situation, try the session again when the coupling storage is resolved.
- VTAM does not have a connection to the coupling facility structure.
- VTAM received an unexpected response from MVS while attempting to access or create the information.

Sense code 08A0

Session Reset: An LU or PU is resetting an LU-LU session.

Bytes 2 and 3 following the sense code contain sense code-specific information.

0000
No specific code applies.

0001
The LU is sending an UNBIND with a reason code of X'0A' (SSCP gone); the identified LU-LU session had to be deactivated because of a forced deactivation of the associated SSCP-PU or SSCP-LU session, for example, because of a DACTPU, DACTLU, or DISCONTACT.

0002
The LU or SCM is sending UNBIND with a reason code of X'0F' (cleanup).

0003
A gateway node is cleaning up the session because a gateway SSCP has directed the gateway node (via NOTIFY) to deactivate the session, for example, a session setup error or session takedown failure has occurred. The gateway node will send UNBIND with a reason code of X'11' (gateway node cleanup).

0004
Reversed FRSN values: The value in the last FRSN Sent field is greater than the value in the current FRSN field in a received TDU GDS variable (no retry). The CP will send an UNBIND with a reason code of X'0F' (Cleanup).

0005
TDU sent out of order: The value in the last FRSN sent field of the current TDU GDS variable is less than the value of the current FRSN field in the TDU GDS variable that immediately preceded it, or is greater than it and the receiver cannot store the out-of-sequence value (no retry). The CP will send an UNBIND with a reason code of X'0F' (Cleanup).

VTAM hint: If this sense code is issued in the IST1097I message group (CP-CP sessions have been deactivated), it is likely that the topology database update (TDU) flowing between the two nodes has been lost. This is probably due to a storage depletion condition on either the sending or receiving end of the TDU flow.

If the CP-CP sessions do not come back up automatically, reactivate the CP-CP session by issuing VARY ACT,ID=*partner_cpname*,IDTYPE=CP. If VTAM is experiencing temporary storage allocation problems, you might want to wait for the condition to clear before attempting to restart the session.

When the CP-CP session is restarted, TDUs will be exchanged so that the missing information in the lost flow will be recovered.

0006
This sense code can be displayed in a VTAM message but is set by another product.

VTAM hint: If this sense code is issued in the IST1097I message group (CP-CP sessions have been deactivated), it is likely that CM/2 is failing the CP-CP session because the flow reduction sequence number (FRSN) in the topology database update (TDU) sent by VTAM is higher than expected by CM/2. Perform the following steps:

1. Delete the entry for the adjacent node from the topology database by issuing the MODIFY TOPO command: F TOPO,ID=cpname,TYPE=FORCE. All links between VTAM and the partner node must be inactive before issuing the MODIFY TOPO command.
2. After deleting the node, reactivate the CP-CP session.

0007
DLUS-DLUR session deactivation (disruptive): LU-LU sessions for DLUR-supported dependent LUs should be reset

0008
DLUS-DLUR session deactivation (non-disruptive): LU-LU sessions for DLUR-supported dependent LUs should not be reset

0009
DLUS-DLUR session deactivation (non-disruptive): protocol violation detected (LU-LU sessions for DLUR-supported dependent LUs should not be reset)

000A
DLUS-DLUR session deactivation (non-disruptive): DLUR should wait for DLUS reactivation of DLUS-DLUR session (LU-LU sessions for DLUR-supported dependent LUs should not be reset)

000C
The DLUS node has received from the DLUR node a FID2 Encapsulation (X'1500') GDS variable with a PIU length field of zero.

Sense code 08A2

Resource active. The requested function must be performed on an inactive resource, but the resource is active.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
RNAA(MOVE) was received for an active resource.

Sense code 08A3

Call security verification failed.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
The callee detected a password mismatch during call security verification.

Sense code 08A4

Token-match exception: partial name matching is unsuccessful during the required find or store operation. The canonical identifier involved in the exception is reported in the FS server report.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
One or more must-match tokens were not specified.

0002
Specified token-match indicators yield multiple directory matches.

Sense code 08A6

Object not found: an exception has occurred when the general server attempted to process the server object, but the server object could not be found.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Server object not found.

Sense code 08A8

Multiple-domain support routing exception: The MDS router in the reporting NAU is unable to perform the required routing for an MDS-MU.

When this SNA report code is used in an SNA condition report (X'1532') GDS variable, the destination NAU name is included in the reported on location name (X'09') subvector and the destination MS application name is included in the reported on agent (X'04') subvector of the condition report.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Destination NAU name unknown. Directory services could not locate the requested destination name.

0002
Directory services unavailable. No routing possible.

0003
MS application program name not recognized.

0004
Use of CPSVCMG session not permitted. The reporting network node has received an MDS-MU over a CPSVCMG session from another network node. These sessions are used for MDS-MUs only between a network node and its served end nodes.

0005
Function not supported by EN destination. The back-level end node destination does not support receipt of MS messages (reported by serving network node).

0006
Function not supported by destination. The back-level destination does not support receipt of MS messages other than MS Capabilities and Alert.

0007
Function not supported by serving NN. The serving network node of the end node destination does not support routing of MS messages (reported by network node performing routing).

0008
Function not supported by EN. The reporting end node has received an MDS-MU with a destination other than itself.

0009
Destination not supported by reporting NN. A network node has received an MDS-MU from another network node that cannot be routed. The destination is not the reporting network node itself nor is it one of the served end nodes.

If the MDS-MU was routed based on nonverified directory information (as indicated by the routing verification indicator in the MDS routing information), the MDS-MU will be returned to the routing network node along with the SNA condition report.

000A
Unrecoverable session failure. The MDS_SEND TP in the reporting node was unable to send the message because of an allocation error. Retries have been exhausted.

000B
Unrecoverable TP failure in remote node. The MDS_SEND TP in the reporting node was unable to send the message because of a TP failure in a remote node. Retries have been exhausted.

000C
MS application program failure. The MDS router in the destination NAU is unable to communicate with the destination MS application program.

000D
Unrecoverable TP failure in reporting node. The MDS router in the reporting node was unable to send the message because of a local TP failure.

000E
Correlation error. An MDS-MU has been received that is not the first for a unit of work (first MDS message indicator in the MDS routing information message is zero), but the agent unit of work correlator is unknown (does not match any active MDS transaction). Also used to report the receipt of a duplicate correlator (MDS-MU with first MDS message indicator is one, but the agent unit of work correlator matches one currently in use).

000F
MS application program congestion. The MDS router in the destination NAU is unable to communicate with the destination MS application program because of local congestion (implementation buffer space for queuing additional MDS-MUs has been exhausted).

0011
MDS HPO not supported by MS application program. The destination MS application program does not support the use of the MDS high performance option.

0012
Unrecoverable failure of user-mode session. MDS has detected an error on a user-mode session (a user-mode session in this context is one with a mode name other than SNASVCMG or CPSVCMG). Retries have been exhausted. Application program data might have been lost.

0013
Session UNBIND notification. The last session to the indicated destination has been deactivated. See product documentation for additional information.

Sense code 08A9

Multiple-domain support transaction failure: The reporting MDS router or MS application program has detected a condition that has impacted an outstanding unit of work (identified by the agent unit of work correlator of the MDS error message).

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
Failure caused by outage of a CPSVCMG session.

0002
Failure caused by outage of an SNASVCMG session. All retries have been exhausted.

0003
Unit of work canceled by reporting MS application program. The unit of work has been canceled because of a timeout in the reporting MS application program.

VTAM hint: For applications using the NetView LU 6.2 transport, the timeout value is determined by the SECONDS parameter on the transport send service, or the RCVREPLY value set by the DEFAULTS command.

0004
Unit of work canceled by reporting MDS Router. The unit of work has been canceled by a garbage-collection timeout in the reporting MDS router.

VTAM hint: For applications using the NetView LU 6.2 transport, this sense code is returned if the timeout value for a request matches that set by MAXREPLY on the DEFAULTS command.

0005
MDS router internal failure. The unit of work has been canceled because of an internal failure in the reporting MDS router.

VTAM hint: For applications using the NetView LU 6.2 transport, this sense code indicates that either the DSI6DST or DSIHPDST task is terminating, or that there was a problem with an internal NetView hashing routine.

0006
MS application internal error. The unit of work has been canceled either because the reporting MS application program was terminated or because another application program served by it was terminated. The type of program termination (normal or abnormal) is not indicated.

0007
MS application router reinitialization. The unit of work has been canceled by the reporting MDS router because of a reinitialization of the application-level router.

Sense code 08AA

Required GDS variable missing: the MS multiple-domain support message unit (MDS MU) is missing a required GDS variable.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

nnnn
Bytes 2 and 3 following the sense code contain the ID of the missing GDS variable.

1212
Control point management services unit X'1212' GDS variable is missing.

1310
DS MU header X'1310' GDS variable is missing.

1311
MDS routing information X'1311' GDS variable is missing.

1532
MDS SNA condition report X'1532' GDS variable is missing.

1549
MDS unit of work X'1549' GDS variable is missing.

80F0
MS capabilities X'80F0' MS major vector is missing.

Sense code 08B2

Data transmission failure: the data transmission between an application program in an SNA MS entry point and an application program in a subentry point was incomplete, causing abnormal termination of the function.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000
No specific code applies.

0001
A timeout has occurred while waiting for transmission of data between the two application programs. For example, a service processor has timed out while waiting to receive data from the main processor.

0002
A timeout has occurred while waiting for transmission of data between two applications.

Sense code 08B5

Network node server not required: Sent by an APPN end node control point to a network node control point (1) to deactivate CP-CP sessions with the NNCP, or (2) to reject a CP-CP session BIND from the NNCP. The end node no longer requires network node services from the receiver.

Note: This sense data value is carried within the X'35' control vector on an UNBIND(Type = X'01') for case (1) above, or on an UNBIND(Type = X'FE') for case (2).

VTAM hint: A possible cause of this error is that the network node server for the CP-CP session attempt is not in the network node server list.

Sense code 08B6

CP-CP Sessions Not Supported: Sent by a network node control point to reject a CP-CP session BIND from another APPN control point; support for CP-CP sessions on that TG was removed since the time when the TG was first activated.

Note: This sense data value is carried within the X'35' control vector on an UNBIND(Type = X'01').

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0000
No specific code applies.

0001
During link activation on a switched link, it was discovered that the partner node does not support CP-CP sessions on this TG.

10XX (request error)

This category indicates that the RU was delivered to the intended NAU component, but could not be interpreted or processed. This condition represents a mismatch of NAU capabilities.

Category and modifier (in hexadecimal):

Sense code 1001

RU data error: Data in the request RU is not acceptable to the receiving component; for example, a character code is not in the set supported, a formatted data field is not acceptable to presentation services, or a value specified in the length field (LL) of a structured field is not valid.

VTAM hint: This code can also be issued if a required name in the request is omitted.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0001
The request contains a subarea address of zero or a subarea address greater than the maximum subarea value within the specified or implied network.

VTAM hint: A possible cause of this error is that a network address cannot be assigned to a dynamic application program when VTAM is trying to build that dynamic application program from a model application program definition.

0002
The network ID specified in the ACTPU is unknown, or is not valid on the link over which the ACTPU was received.

0003
Isolated pacing message format error: An incorrectly formatted isolated pacing message was received.

0005
An RNAA Type 4 was received in which the local address field length is greater than one. The implementation does not support a length other than one.

0006
An RNAA Type 4 was received in which the link station address field length is greater than one. The implementation does not support a length other than one.

0007
On BFCINIT the network name portion of the network-qualified name field has a format error.

0008
A character code that is not valid was found.

0009
The formatted data field is unacceptable to presentation services.

000A
A length field for a structured field that is not valid was found.

000B
The value in the name length field is not valid.

000C
The value in the cryptography length field is too great.

000D
The URC length field is not valid.

000E
The control vector length field is inconsistent with the control vector data.

000F
A PLU or SLU role specification encoding is not valid.

0010
The value in the user data length field is not valid.

0020
Too many session keys are present.

0021
A control vector or session key data is not valid.

0022
A BIND image in a session services RU is not valid.

0023
A device characteristics field is not valid.

0024
A BIND or +RSP(BIND) that was not for LU Type 6.2 and not in extended format was received at an intermediate APPN network node. The session is terminated.

0026
The length of GDS variable within the request RU is not valid.

0027
A GDS variable within a locate is not valid.

0030
Control vector ambiguity: The request contains two or more conflicting control vectors. Generally the two control vectors have the same key. However, there are cases where a new control vector key supersedes an old one. In this case, two control vectors with different keys but no other distinguishing

data (such as network ID) could be ambiguous. An example is a SETCV to a gateway node with both a VR ID list control vector (control vector X'1B') and a route parameters control vector (control vector X'4E') for the same network.

0033
The name of the deciphering CP in a cryptography (X'63') control vector does not match the name of the receiving CP(PLU).

0034
A topology data update was received across an APPN subnetwork link carrying topology information about an adjacent subnet.

VTAM hint: Information that was not valid was received in a topology database update (TDU) over an APPN subnetwork link. This sense code is set only by a border node during the initial topology exchange after CP-CP sessions are established over an APPN subnetwork link. If the non-native node sends a TDU containing more topology information that its own X'44'/X'45' control vector pair, then the sense code is set. A dump from both nodes should be taken for problem determination.

0035
A logon command was entered using a format different from that specified at system-definition time for the USS table.

0036
The message authentication code received in the RU did not match the one generated by the receiver for that RU.

0037
The data manipulation header contained data that was not valid.

0038
The data manipulation header contained a length that was not valid.

hnnn
Where *h*≥8; that is, the high-order bit in Byte 2 is set to one. The 15 low-order bits of Bytes 2 and 3 contain a binary count that indexes (zero-origin) the first byte of the field found to be in error.

Sense code 1002

RU length error: The request RU was too long or too short.

Sense code 1003

Function not supported: The function requested is not supported. The function might have been specified by a formatted request code, a field in an RU, or a control character.

Note: Numbers 0001 and 0002 are also assigned for implementation. See the implementation documentation for details of use.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

VTAM hint: If resources are not activating correctly when a new NCP is activated, either rename the new NCP or use another method to make sure that the old resource resolution table (RRT) is replaced with the new RRT.

0001
The half-session receiving the request did not perform the function because it is not capable of doing so. The requesting half-session requested a function that the receiver does not support, and the receiver did not specify that it was capable of supporting the function at session activation; consequently, there is an apparent mismatch of half-session capabilities.

Note: This is to cover a system error. For example, if the PU receiving a SETCV (vector key=X'15') is not a gateway PU; that is, if the PU did not indicate in the ACTPU response that it is a gateway PU, the PU reports to the SSCP that sent the SETCV that there is an apparent mismatch of half-session capabilities.

0002
The half-session receiving the request did not perform the function, though it is capable of doing so. The requesting half-session did not specify at session activation that it was capable of supporting the function; consequently, there is an apparent mismatch of half-session capabilities.

Note: This is to cover a system error. For example, if the SSCP sending a SETCV (vector key=X'15') is not known to the receiving PU as a gateway SSCP; that is, the SSCP did not indicate in ACTPU that it is a gateway SSCP, the PU reports a mismatch of capabilities.

0003
The component received an unsupported normal-flow DFC command.

0004
The component received an unsupported expedited-flow DFC command. For example, the LU 6.2 half-session might have received a SIGNAL RU when its local conversation style is full-duplex. (However, the half-session rejects the SIGNAL only if it is for the current bracket. Early SIGNALs are held for the correct bracket by saving the SIGNAL value until the correct BB arrives.)

0005
The component received a network control command during an LU-SSCP session.

0006
The component received an unsupported session control command during an LU-SSCP session.

0007
The component received an unsupported data flow control command with LU-SSCP session specified.

0008
Broadcast search with reservation: An NNCP received a broadcast search request with reservation.

0009
Initiate type: The initiate type requested in the CDINIT GDS variable or INIT_OTHER_CD GDS variable is not supported at the receiver.

000A
Session polarity: The session polarity requested in the CDINIT GDS variable is not supported at the receiver.

000B
A BIND specifying delayed request mode was received from a non-6.2 Type LU, but delayed request mode is not supported in the receiver.

000C
A stand-alone BIND is received from a node that is served by an SSCP that does not support stand-alone BINDs.

000D
The function identified in the request is not supported by the processing application transaction program.

0010
The RU is not known to session services.

0011
A session key is not supported.

0012
A control vector is not supported.

0014
Cryptography is not supported but a nonzero length was specified for the cryptography key.

0015
Queuing not supported for a controller session.

0016
Service parameter not supported. When this SNA report code is used in an SNA condition report, it is accompanied by a supplemental report identifying the service parameter triplet (or triplets) that was not supported.

0017
Service parameter level not supported. When this SNA report code is used in an SNA condition report, it is accompanied by a supplemental report identifying the service parameter triplet (or triplets) that was not supported.

0018
Destination-role function not supported. When this SNA report code is used in an SNA condition report, it is accompanied by a structure report identifying the structure and containing the contents that specified the unsupported function. Whenever the structure report is not sufficient to identify the unsupported functions, the supplemental report might also be present.

0019
All-role function not supported. When this SNA report code is used in an SNA condition report, it is accompanied by a structure report identifying the structure and containing the contents that specified the unsupported function. Whenever the structure report is not sufficient to identify the unsupported functions, the supplemental report might also be present.

001B
Unable to initiate agent.

001C
Function conflicts with Format Set 1 encodings. When this SNA report code is used in an SNA condition report, it is accompanied by a structure report identifying the structure and containing the contents that specified the conflicting function.

001F
Multiple-destination traffic not supported. The reporting location is a specialized, end-only role implementation that supports single-destination traffic only.

0020
A session initiation request specified an OLU and DLU that are the same LU. An LU that does not use VTAM LU 6.2 API cannot establish a session with itself.

0021
There is a mismatch between session initiation request type and LU type (independent or dependent). For example, a session initiation request other than BFINIT identifies an independent LU as a session partner.

VTAM hint: Ensure that the PU name and CPNAME operand have unique names in the PU definition statement of the switched major node definition.

0023
A session initiation request requiring Extended Session Services NNS Support was received at an EN that does not have this service available to it.

0025
The component received a NOTIFY request whose type is not supported.

0027
LU type is not supported.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product. See the appropriate product-specific manual for further information.

0036
The network node server received a NOTIFY request whose type is not supported by the DLU.

0037
Request received is inappropriate for the receiving type of network addressable unit.

0039
A third-party-initiated session request specified an ILU (initiating LU) and a DLU (destination LU) that are the same LU. An application cannot initiate a third-party-initiated session to itself.

6002
The resource identified by the destination program name (DPN) is not supported.

6003
The resource identified by the primary resource name (PRN) is not supported.

Note: This sense code can also be used instead of sense code X'0826'.

Sense code 1005

Parameter error: A parameter modifying a control function is not valid, or outside the range allowed by the receiver.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
For NMVT, the address type field in an SNA address list subvector does not match the address type required by the command subvector.

0003
Number of element addresses requested was not valid.

0004
Display type was requested was not valid.

0005
Storage length for display type requested was not valid.

0006
Storage address was not valid; out of specified range.

0007
The command in a request change control MS major vector is incompatible with the SNA/FS server instruction.

0010
A new backup focal point name was supplied when we are supposed to keep the current backup focal point information.

Sense code 1006

Required field or parameter is missing.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

VTAM Information: When VTAM receives this sense code for a session initiation, it continues searching through the adjacent SSCP table until the destination LU is found or routing is exhausted.

0001
One or more required COS names were omitted.

0002
A required name was omitted.

0003
A required network identifier was omitted.

0004
A required session key was omitted.

0005
A required control vector was omitted.

0006
A required subfield of a control vector was omitted.

0007
The TG number field was omitted.

0008
The specific ID (IDNUM) was omitted.

0009
A required GDS variable is missing.

Sense code 1007

Category not supported: DFC, SC, NC, or FMD request was received by a half-session not supporting any requests in that category; or an NS request Byte 0 was not set to a defined value, or Byte 1 was not set to an NS category supported by the receiver.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
NS header received was not valid. An NS request Byte 0 was not set to a defined value.

Sense code 1008

Invalid FM header: The FM header was not understood or translatable by the receiver, or an FM header was expected but not present. For LU 6.2, this sense code is sent in FMH-7 or UNBIND.

Table 1 on page 104 shows the usage of the allowed values by LU type.

Table 1. Usage of hexadecimal 1008 sense code specific information by LU type

Range	LU 1	LU 4	LU 6.1	LU 6.2
0801–0824	X	X		
0825	X			
0826–082A	X	X		
2001–200D	X	X		
200E	X	X	X	
200F–201C	X	X		
201D				X
4001–400E	X	X		
6000				X
6001,6004			X	
6005			X	X
6006–6008			X	
6009			X	X
600A			X	
600B			X	X
600C–6010			X	
6011–6034				X

Table 1. Usage of hexadecimal 1008 sense code specific information by LU type (continued)				
Range	**LU 1**	**LU 4**	**LU 6.1**	**LU 6.2**
6040			X	X
6041				X
6046				X
6047				X
6048				X
C000–C003			X	

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0801
The function code parameters are not valid.

0803
The forms functions cannot be performed.

0805
The copy function cannot be performed.

0806
Compaction table outside the supported set: The number of master characters is not within the valid range.

0807
The PDIR (peripheral data information record) identifier is not valid.

0808
The printer train function cannot be performed.

0809
The FCB (forms control block) load function cannot be performed.

080A
The FCB (forms control block) load function is not supported.

080B
The compaction table name is not valid.

080C
The ACCESS is not valid.

080D
The RECLEN is not valid.

080E
The NUMRECS is not valid.

080F
The data set is in use.

0810
The data set cannot be found.

0811
The password is not valid.

0812
The function is not allowed for the destination or for the data set.

0813
The record is too long.

0814
The data set is full.

0815
The RECID is not valid.

0817
The VOLID format is not valid.

0818
The maximum number of logical records per chain is exceeded.

0819
The data set exists.

081A
No space is available.

081B
The VOLID is not valid.

081C
The DSACCESS is not valid.

081D
The RECTYPE is not valid **or** the data set cannot be found.

081E
The resolution space is insufficient.

081F
The key technique is not valid.

0820
The key displacement is not valid.

0821
The key is not valid.

0822
There is an not valid N (number of records).

0823
The KEYIND is not valid.

0824
The SERID is not valid.

0825
Disk error: An error was detected while reading from, or writing on, the disk.

0826
The RECID format is not valid.

0827
The password has not been supplied.

0828
The record ID has not been supplied.

0829
The volume ID has not been supplied.

082A
The PGMNAME is not valid.

2001
The destination (active) is not valid.

2002
The destination (inactive) is not valid.

2003
The destination (suspended) is not valid.

2004
The suspend-resume sequence is not valid.

2005
There has been an interruption level violation.

2006
The resume properties are not valid.

2007
The destination is not available.

2008
The end sequence is not valid.

2009
The FM header length is not valid.

200A
Field setting is not valid: The reserved field is set to one or the setting is not defined.

200B
Destination is not valid: The destination does not exist.

200C
The ERCL is not valid.

200D
The data stream profile (DST) is not valid.

200E
Concatenation indicator is not valid: The concatenation indicator is on, but concatenation is not allowed.

200F
FM data is not allowed for the header.

2010
The FM header set specified in the BIND has been violated.

2014
The FM header was not sent concatenated.

2019
The stack reference indicator (SRI) is not valid.

201A
The CMI modification could not be accepted.

201B
The CPI modification could not be accepted.

201C
The ECRL modification could not be accepted.

201D
FM header and associated data mismatch: The FM header indicated that associated data would or would not follow (for example, FM Header 7 followed by log data, or FM Header 5 followed by program-initialization parameters), but this indication was in error; or a previously received RU [for example, -RSP(X'0846')] implied that an FM header would follow, but none was received.

4001
FM header type for this LU is not valid: The type of the FM header is other than five, seven, or 12.

4002
The FMH code is not valid.

4003
Compression is not supported.

4004
Compaction is not supported.

4005
Basic exchange is not supported.

4006
Only basic exchange is supported.

4007
The medium is not supported.

4008
There has been a code selection compression violation.

4009
FMHC is not supported.

400A
Demand select is not supported.

400B
DSNAME is not supported.

400C
The media subaddress field is not valid.

400D
There are insufficient resources to perform the requested function.

400E
Data stream profile (DSP) select is not supported.

6000
FM header length not correct: The value in the FM header length field differs from the sum of the lengths of the subfields of the FM header.

6001
The deblocking algorithm (DBA) is not valid.

6004
The queue name length is not valid.

6005
Access security information length field not correct: The value in the access security information length field differs from the sum of the lengths of the access security information subfields.

6006
The data stream profile (DSP) is not valid.

6007
The FMH-7 is not preceded by a negative response carrying sense code X'0846'.

6008
The attach access code is not valid.

6009
Parameter length is not valid: The field that specifies the length of fixed-length parameters has a setting that is not valid.

600A
This is not the first FMH-5, the interchange unit type is not the same as the old, and the interchange unit end indicator is off.

600B
Unrecognized FM header command code: The partner LU received an FM header command code that it does not recognize. For LU 6.2, this sense data is sent only in FMH-7.

600C
A null sequence field is required.

600D
User-to-user program transition is not allowed.

600E
User to non-SNA defined program transition is not allowed.

600F
The FMH-5 reset attached program (RAP) was not sent properly.

6010
The FMH-5 reset attached program (RAP) was sent with an inactive attach register.

6011
Logical unit of work (LUW) not valid: The LUW length field (in a compare states GDS variable or an FMH-5) is incorrect, or the length field is not valid, or a LUW ID is not present but is required by the setting of the synchronization level field.

6021
Transaction program name not recognized: The FMH-5 attach command specifies a transaction program name that the receiver does not recognize. This sense data is sent only in FMH-7.

6031
PIP not allowed: The FMH-5 attach command specifies that program initialization parameter (PIP) data is present, but the receiver does not support PIP data for the specified transaction program. This sense data is sent only in FMH-7.

6032
PIP not specified correctly: The FMH-5 attach command specifies a transaction program name that requires program initialization parameter (PIP) data, and either the FMH-5 specifies PIP data is not present or the number of PIP subfields present does not agree with the number required for the program. This sense data is sent only in FMH-7.

6034
Conversation type mismatch: The FMH-5 attach command specifies a conversation type that the receiver does not support for the specified transaction program. This sense data is sent only in FMH-7.

6040
Attach parameter is not valid: A parameter in the FMH-5 attach command conflicts with the statement of LU capability previously provided in the BIND negotiation.

6041
Synchronization level not supported: The FMH-5 attach command specifies a synchronization level that the receiver does not support for the specified transaction program. This sense data is sent only in FMH-7.

6042
Reconnection not supported: The FMH-5 attach command specifies reconnection support, but the receiver does not support reconnection for the specified transaction program. This sense data is sent only in FMH-7.

6043
Unable to reconnect transaction program—no retry: The FMH-5 reconnect command specifies the conversation correlator of a transaction program to which the receiver cannot reconnect. The condition is not temporary. This sense data is sent only in FMH-7.

6044
Unable to reconnect transaction program—retry allowed: The FMH-5 reconnect command specifies the conversation correlator of a transaction program to which the receiver cannot reconnect. The condition is temporary. This sense data is sent only in FMH-7.

6046
An SNA/DS transaction program is unable to allocate a conversation with an SNA/DS partner.

6047
An SNA/DS transaction program in conversation with an adjacent SNA/DS transaction program has detected from LU 6.2 PS a return code of resource_failure.

6048
An SNA/DS transaction program in conversation with an adjacent SNA/DS transaction program has detected from LU 6.2 PS a return code of deallocate type (abend).

6050
For the receiver, one of the following conditions exists:

- Extended security bit is on and GDS variable X'12F6' does not immediately follow the attach FMH-5 and PIP data.
- Extended security bit is off and GDS variable X'12F6' follows the attach FMH-5.

For the sender, one of the following conditions exist:

- The partner responded to the attach with any data other than an FMH7 or an authenticator reply (GDS id X'12F8').
- The authenticator reply subfield (X'FF85') is absent.
- A subfield occurs more than once.

6051
One of the following conditions exist:

- The length of the GDS variable is incorrect. The length must be greater than zero and must equal to (*length_field_value -2*).
- An unidentified subfield is present in the GDS variable.
- The total length of a subfield is not equal to the value in its length field minus 2.

6053
The length of the GDS variable is incorrect. It is the responsibility of the application to ensure that the GDS variable length is correct. For the sender, the length must be greater than or equal to two and must equal the value in the length field.

6054
For the receiver, the extended security bit is on and either old FMH-5 security bits are on or the old access security information fields are present. For the sender, the authenticator reply fails the checks applied by the security manager. (Purge ID from Signed On To list.)

6056
The partner responded to the attach with any data other than an FMH7 or an authentication token (GDS variable X'12F6').

6057
The authentication token GDS requested that additional token exchanges be handled via the distributed authentication service TP. However, the FMH5 did not contain a valid conversation correlator.

C000
The header is not supported.

C001
The header length is not valid.

C002
There has been a logical message services block-level error.

C003
There is a version ID mismatch.

Sense code 1009

Format group not selected: No format group was selected before issuing a present absolute or present relative format structured field to a display.

Sense code 100A

Unknown user name.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The specified operations management served application name is not registered with operations management. The operations management served application name is specified in the DAN X'50' subfield of the name list X'06' subvector which is contained in the R and TI X'154D'.

Sense code 100B

Format exception.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
Required structure absent. When this SNA report code is used in an SNA condition report, it is accompanied by a structure report that identifies the absent structure. For example, the destination application name is missing in the MDS_MU received.

0002
Precluded structure present. This SNA report code is accompanied by a structure report that identifies the precluded structure.

0003
Multiple occurrences of a nonrepeatable structure. This SNA report code is accompanied by a structure report that identifies and contains the second occurrence of the structure.

0004
Excess occurrences of a repeatable structure. This SNA report code is accompanied by a structure report that identifies and contains the occurrence of the structure that exceeded the maximum number of occurrences.

0005
Unrecognized structure present where precluded. This SNA report code is accompanied by a structure report that identifies and contains the precluded unrecognized structure, plus a sibling list of all the allowed structures.

0006
Length outside specified range. This code assumes that the length arithmetic balances and that the sender intended to send the structure at that length. This SNA report code is accompanied by a structure report that identifies and contains the header of the excessively long structure plus a supplemental report that contains the allowed maximum length.

0007
Length exception. Length arithmetic is out of balance. This SNA report code is accompanied by a structure report that identifies and contains the header of the structure that exceeded its parent's boundary.

0008
Required combination of structures absent. This SNA report code is accompanied by structure reports that identify the structures that make up the combination, indicating for each whether it was present or absent.

0009
Precluded combination of structures present. This SNA report code is accompanied by structure reports that identify the structures that make up the precluded combination.

000A
Required combination of structures and data values absent. This SNA report code is accompanied by structure reports that identify the structures and data values that are present, plus structure reports that identify the absent structures needed to complete the combination.

000B
Precluded combination of structures and data values present. This SNA report code is accompanied by structure reports that identify the structures and data values that make up the precluded combination.

000C
Unknown or unsupported data value. This SNA report code is accompanied by a structure report that identifies the structure and contains the unknown or unsupported data value.

000D
Incompatible data values. This SNA report code is accompanied by structure reports that identify the structures and contain the incompatible data values.

000E
Precluded character present. This SNA report code is accompanied by a structure report that identifies the structure, indicates the byte offset of the offending byte, and includes the byte containing the precluded code point.

000F
Data-value out of range. This SNA report code is accompanied by a structure report that identifies the structure and contains the offending data value, plus a supplemental report that contains the maximum value allowed within the range (if a maximum range value is applicable).

0010
Segmentation present where precluded. This SNA report code is accompanied by a structure report that identifies the structure that should not have been segmented.

0011
Precluded data value. This SNA report code is accompanied by a structure report that identifies the structure and contains the offending data value.

0012
Recognized but unsupported structure. This SNA report code is accompanied by a structure report that identifies the structure.

0013
None of several possible structures found. This SNA report code is accompanied by a structure report that identifies the parent of the absent structure and might contain an unrecognized structure that was found in the place of the absent structure. The structure report also contains a sibling list of the possible structures.

0014
Incorrect order of child structures found. This SNA report code is accompanied by a structure report that identifies the parent of the incorrectly ordered child structures.

Sense code 100C

Unrecognized message unit.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The received byte stream could not be identified by the receiving SNA component.

Sense code 100D

Request inconsistency: the control information provided for the request is not consistent with other information in the request.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
Server object size is incompatible with service level.

0002
A reply DTMU was received before completing a three-way responsibility flow in an SNA/DS request. Retry is allowed.

Sense code 100E

Directing exception: a node is unable to perform the required directing or redirecting function for a request as a result of insufficient directory support, or incompatibility between TP name and presence/absence of a user name.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
Agent name known but not supported for specified user destination.

0002
Agent name known but not supported for specified node destination.

0003
Agent name is known at this DSU but is not available.

Sense code 100F

Improper SNA/DS usage of LU 6.2.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
An SNA/DS transaction program in conversation with an adjacent SNA/DS transaction program has detected an improper sequence of LU 6.2 basic conversation verbs.

Sense code 1010

Error on locate search or CP capabilities message detected.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
Unrecoverable error, such as a duplicate control vector, was detected.

0001
A broadcast search resulted in two or more conflicting positive replies that differ on the CP owning the target resource. Multiple positive replies are acceptable, as long as all indicate the same owning CP.

0003
An error was detected that prevented the exchange of CP capabilities. Recovery might be attempted.

0004
Unrecoverable error on CP Capabilities GDS variable exchange prevented its initiation or completion on a contention-winner CP-CP session.

0005
The intersubnetwork Locate failed because an entry for the destination network ID does not exist in the border node subnetwork list.

VTAM hint: This sense code can be displayed in a VTAM message, but is set by another product.

1000
Length error in CP capabilities GDS variable.

1002
A GDS variable that is not valid was received when the CP capabilities (X'12C1') GDS variable was expected.

VTAM hint: VTAM detects this condition during either contention-winner or the contention-loser CP-CP session activation. VTAM deactivates the CP-CP session.

4004
Incomplete negative or neutral reply received on a search or reservation indicated on Broadcast or "All" specified on a directed search.

5002
No CD-Initiate GDS variable returned on a search request.

5006
Session polarity or initiate type value received in CD-Initiate GDS variable not supported.

500A
Mode name length error in CD-Initiate GDS variable.

A002
Find GDS variable not present on Locate search request.

B080
Command parameters (X'80') control vector not present on found GDS variable.

Sense code 1011

RNAA request error: The RNAA must be rejected because there is a mismatch between sending and receiving system definitions, or capabilities.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
No available pre-ENA addresses: Reject an RNAA that requests an address that is pre-ENA compatible, and there are no pre-ENA addresses available.

0002
RNAA takeover error: In a takeover situation, a system definition mismatch was detected between the "old" SSCP and the SSCP taking over. For example, if the LU name field in the RNAA is not the same as the LU name field in the logical unit block (LUB), the RNAA is rejected. If an existing LU with the same local address is found, but the LU is generated (instead of DR-added), the RNAA is rejected. Also, if the adjacent link station (ALS) name given in the RNAA does not agree with the ALS name given in the common physical unit block (CUB), the RNAA is rejected.

0003
NETID not valid: If the NETID field in the RNAA is not the same as the native network ID, the RNAA is rejected. There is likely a mismatch between the PU Type 4 and SSCP system definitions.

0004
PU or LU type not valid: If the PU to which the LUs are to be added is not Type 1 or Type 2, the RNAA is rejected. The SSCP attempts to add an LU to a PU, but NCP has defined that PU as a PU Type 4. The second situation is if the SSCP sent an RNAA Type X'00' or X'05' with a PU or LU specified. This is an RU-NAU mismatch caused by an SSCP-NCP definition mismatch.

0005
MAXSUBA required for pre-ENA address assignment: If MAXSUBA is not specified and an RNAA requesting a pre-ENA address is received, the RNAA is rejected.

Sense code 1012

SNA/DS receiver exception MU format exception: Parsing or building of the SNA/DS receiver exception MU format was unsuccessful.

Sense code 1013

Unknown server parameters: The specified parameters are not recognized by the server.

Sense code 1014

Control vector error on a directory services GDS variable.

Bytes 2 and 3 following the sense code contain sense code specific information.

003C
Missing associated resource entry (X'3C') control vector on find or found.

003D
Missing directory entry (X'3D') control vector on find or found.

0060
Missing CV60 on LOCATE GDS variable.

0080
Control vector not valid.

023C
Conflicting directory entry, or associated resource entry (X'3C') control vector not valid.

502B
No RSCV received from a network node server.

502C
No COS/TPF control vector received in a CD-Initiate reply from a network node server.

502D
The COS/TPF control vector received on the BIND is different from that on the corresponding Locate.

VTAM hint: A dump should be taken for problem determination.

5046
TG vectors not present in a CD-Initiate from an end node OLU or DLU.

VTAM hint: This sense code can also be set by AS/400 when an attempt to establish a session from one AS/400 to a second AS/400 across a VTAM network fails. Sessions across three different networks using APPN links are not supported in VTAM. See the information about common APPN problems in the z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this problem.

A080
Missing command parameters (X'80') control vector on find.

A082
Missing search argument directory entry (X'82') control vector on find.

B280
A found from an end node indicated the directory entry for a located resource was a wild-card entry.

Sense code 1015

XID Length Error: The XID3 was too long or too short. Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The received XID3 has fewer than 29 bytes.

0002
There is a mismatch between the number of bytes specified in the length field of XID3 and the actual length of the received XID3.

Sense code 1016

XID Format 3 parameter error: Data in the XID3 is not acceptable to the receiving component because the value in the received XID3 field, whose byte and bit offset is specified by the XID negotiation error (X'22') control vector (which also carries this sense data), is inconsistent with the corresponding field in the sent XID3.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The field in the received XID3 that specifies the maximum number of I-frames that the sender can receive before acknowledgment is set to zero.

0002
The adjacent node has been inconsistent in its request for ACTPU. In a nonactivation XID3 exchange, it has changed the value of the ACTPU suppression indicator sent in the previous XID3 exchange.

0003
The field in the received XID3 that specifies the maximum BTU length that the sender can receive is set to less than 99 bytes, the minimum required.

0004
The received XID was not XID Format 3 when XID Format 3 was expected.

0005
The adjacent node does not support BIND segment generation but does support receipt of BIND segments. Any T2.1 node supporting receipt of BIND segments must also support generation of BIND segments.

0006
The adjacent node is an end node, does not support BIND segment receipt, and has a maximum BTU size of less than 265, the minimum required in this case.

0007
The adjacent node is a network node, does not support BIND segment receipt, and has a maximum BTU size of less than 521, the minimum size required in this case.

0008
The adjacent node has changed its networking capabilities in an XID3 from those declared in the previous negotiation-proceeding or nonactivation XID3. A node may not change from an end node to a network node or from a network node to an end node in two different negotiation-proceeding or nonactivation XID3s.

0009
The adjacent node is an APPN network node, does not provide CP services, and supports CP-CP sessions, a combination not allowed.

000A
During a nonactivation XID3 exchange, the adjacent node has changed the TG number that was negotiated during the activation exchange.

000B
The adjacent node is the TG number negotiation winner and designates a TG number that the receiving node cannot allocate to this connection. When parallel TGs are supported between the two nodes, zero is always such a number.

Tip:

- This sense code occurs when two VTAMs are attached by a 3172 token ring and channel-to-channel connections or any other type of connection in parallel to a 3172 connection. After deactivation of a VTAM node with 3172 connections, you should do one of the following actions:
  - Wait at least four minutes before attempting to restart the failed VTAM.

- Attempt reattachment of the 3172 connections to adjacent nodes first to prevent TG number contention.

- If you receive this sense code in message IST1085I and the PU name in the preceding IST590I message is an Enterprise Extender (EE) PU, this connection traverses EE. If this connection traverses EE, a duplicate CP name might be in the network. From the host where the 1016000B sense code was received in message IST1085I, issue a **DISPLAY EE,CPNAME=** command, where CPNAME specifies the resource name from the IST1085I message. This command will show information about the CP with the active EE connection.

000C
The adjacent node is an APPN network node that does not support BIND segment generation, and this node has a maximum BTU receive size of less than 521. This node might, therefore, be unable to receive a BIND with RSCV from the adjacent network node.

000D
The adjacent node indicates that it does not support the SDLC command/response profile in its XID3. This is the only command/response profile supported by APPN and LEN nodes.

000E
Different product set IDs have been given in the product set ID (X'10') control vectors appended to two different received XID3s from the same adjacent node.

000F
The link station roles specified in the sent and received negotiation-proceeding XID3s are not compatible. To activate a connection, one node must contain a primary link station; the other, a secondary link station.

0010
The support of combined asynchronous balanced mode link stations indicated in the sent and received negotiation-proceeding XID3s is not in agreement.

0011
A received XID3 indicates an attempt to activate multiple connections has been made when parallel transmission groups are not supported between the two nodes involved in the XID exchange.

0012
The adjacent node has sent the network name (X'0E', CP name) control vector in XID3 but indicates it does not support the exchange state indicators.

0013
The DLC type indicated in the sent and received negotiation-proceeding XID3s is not in agreement.

0016
This TG is predefined in this node (range 1–20) but the TG number received in the XID3 from the adjacent node is not the same.

Tip: If you receive this sense code while you are trying to establish a connection with a dynamic EE PU, the dialing side of the connection receives an INOP notification. The cause of the problem might be that none of the TGNs specified on the EE model PU are available.

0018
The adjacent node is an APPN node but does not support adaptive BIND pacing as a sender and receiver.

001A
The adjacent node is inconsistent in its support of parallel TGs. Support of parallel TGs between two nodes cannot change either in link-activation XID exchanges on different TGs or in successive XID exchanges on the same TG.

001B
The adjacent node provides or requests CP services but does not support CP-CP sessions; for example, Bytes 8–9, bits 10–11 of the received negotiation-proceeding XID3 were set to ten, a setting combination not allowed for T2.1 nodes.

001F
The setting of the intersubnetwork link indicator of the TG descriptor control vector received in XID3 is inconsistent with the receiving node system definition. This sense data value is issued only if both sender and receiver support the setting of this bit.

0021
During a negotiation-proceeding XID3 exchange, one node specifies in the HPR capabilities (X'61') control vector that error recovery is required, but the other node specifies no error recovery is required. HPR protocols will not be used on this TG. (This sense data is not carried in the XID negotiation error (X'22') control vector.)

Tip: The link activated as a non-HPR link due to a disagreement between the link partners on the level of error recovery procedures (ERP) to be used. Check the value of the LLERP parameter associated with the VTAM PU, as well as the level of ERP supported for that DLC type by the link partner.

0022
The adjacent node is an HPR node (that is, it included an HPR capabilities (X'61') control vector in XID3), but is specified a maximum BTU size less than 768.

Tip: This sense code can also be issued at the following times:

- At XID time for a Local SNA (CDLC) connection if the maximum PIU size (a factor of the IOBUF size multiplied by the MAXBFRU value) is less than 525 bytes.
- At XID time for a TCP/IP CDLC connection if the product of the write_buffers times write_size, specified on the DEVICE statement, is larger than the read capacity on the read side.

0023
The adjacent node is an HPR node (that is, it included an HPR capabilities (X'61') control vector in XID3), but it specified an ANR label length that was not valid (for example, less than one or greater than eight).

0024
The adjacent node is an HPR node (for example, it included an HPR Capabilities (X'61') control vector in XID3), but the receiving node detected that it specified a CP NCE identifier length that was not valid (for example, less than one or greater than eight).

0025
The adjacent node is an HPR node (for example, it included an HPR Capabilities (X'61') control vector in XID3), but the receiving node detected that it specified a route setup NCE identifier length that was not valid (for example, less than one or greater than eight).

0026
The adjacent node is an HPR node (for example, it included an HPR Capabilities (X'61') control vector in XID3), but the receiving node detected that the length of the HPR Transport Tower (X'81') subfield of the control vector is inconsistent with the length of a field included in the subfield.

0031
The link being activated by this node requires the link to support HPR, be RTP capable, and support the control flows over RTP tower. The adjacent node has indicated that it does not support HPR for this link.

0032
The link being activated by this node requires the link to support HPR, be RTP capable, and support the control flows over RTP tower. The adjacent node has indicated that this link is not RTP capable.

0033
The link being activated by this node requires the link to support HPR, be RTP capable, and support the control flows over RTP tower. The adjacent node has indicated that it does not support control flows over RTP for this link.

0034
The link being activated by this node requires the support of logical data link control (LDLC) during XID exchange for this link. The adjacent node has indicated that it does not support LDLC for this link.

0035
A negotiable or zero TG number was received in XID3, but multiple links are defined between the switched ports. Use of predefined TG numbers is required.

0047
The link being activated by this node requires the link to support HPR, be RTP capable, and support the control flows over Enterprise Extender. The adjacent node has indicated that this link is not RTP capable.

Sense code 1018

MU sequence exception: An SNA/DS transaction program detected an improper sequence of SNA/DS MUs.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0001
A DMU has been received, but the MU_id has already been terminated.

0002
The MU_id state received from the partner is incompatible with the state in the MU_id registry.

0004
A previous terminate conversation indication has been ignored.

0005
An RRMU was received but was not followed by a change_direction indicator (the receive_and_wait verb issued after receiving the RRMU, returned something other than what_received=send).

Sense code 1019

Restart byte position not valid.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0001
The restart byte position value specified in the DCMU is greater than one plus the value of the last byte received in the CRMU.

0002
The receiver does not support the byte-count restart elective, and the restart byte position value specified in the DCMU is not the beginning of the LLid structure following the last successfully received LLid structure.

0003
The receiver supports the byte-count restart elective, and the restart byte position value specified in the DCMU is not equal to one and is less than or equal to the last byte received value specified in the CRMU.

Sense code 101A

Control vector sequence not valid: A control vector was found containing a key that was invalid for the position of the control vector within a TDU.

0000
No specific code applies.

nnmm
Byte 2 following the sense code contains the key (nn) of the vector previous to the one in error; Byte 3 contains the key (mm) of the vector in error.

Sense code 101C

Data received not valid.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
Alteration of input data not allowed.

Sense code 101D

Insufficient Length: The length of the received signal is insufficient to contain additional required fields.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000
No specific code applies.

0001
A BIND or RSP(BIND) was received that was too large to be extended. The BIND was rejected.

0002
An UNBIND was received that was too large to be extended. An UNBIND cleanup is sent on both session stages.

Sense code 101E

Capabilities mismatch. Sent when the control point capabilities of the adjacent node are deemed unacceptable.

Bytes 2 and 3 following the sense code contain sense code specific information.

nnnn
Bytes 2 and 3 contain a binary count that bit indexes (zero-origin) the first unacceptable subfield within the support indicators subfield of the X'12C1' CP capabilities GDS variable.

VTAM hint: See *SNA Formats* or *SNA Network Product Formats* for a description of the CP capabilities GDS variable.

20XX (state error)

This category indicates a sequence-number error, or an RH or RU that is not allowed for the receiver current session control or data flow control state. These errors prevent delivery of the request to the intended component.

Category and modifier (in hexadecimal):

Sense code 2001

Sequence number: Sequence number received on normal-flow request was not one greater than the last.

Sense code 2002

Chaining: Error in the sequence of the chain indicator settings (BCI, ECI), such as first, middle, first.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The receiver received a middle or end-chain request when in the in-chain state.

0002
The receiver received a begin-chain request when in the in-chain state.

Sense code 2003

Bracket: Error resulting from failure of sender to enforce bracket rules for session. (This error does not apply to contention or race conditions.)

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The receiver received a begin-bracket request before receiving a response to its own previously sent begin-bracket request.

0002
The receiver received a begin-bracket request not specifying begin-bracket when in the between-bracket state.

0003
The receiver received an out-of-sequence LUSTAT command.

Sense code 2004

Direction: Error resulting from a normal-flow request received while the half-duplex flip-flop state was not receive.

Sense code 2005

Data traffic reset: An FMD or normal-flow DFC request received by a half-session whose session activation state was active, but whose data traffic state was not active.

Sense code 2006

Data traffic quiesced: An FMD or DFC request received from a half-session that has sent QUIESCE COMPLETE or SHUTDOWN COMPLETE and has not responded to RELEASE QUIESCE.

Sense code 2007

Data traffic not reset: A session control request (for example, STSN), allowed only while the data traffic state is reset, was received while the data traffic state was not reset.

Sense code 2008

No begin bracket: An FMD request specifying BBI=BB was received after the receiver had previously received a BRACKET INITIATION STOPPED request.

Sense code 2009

Session control protocol violation: An SC protocol has been violated; a request, allowed only after a successful exchange of an SC request and its associated positive response, has been received before such successful exchange has occurred (for example, an FMD request has preceded a required cryptography verification request). The request code of the particular SC request or response required, or X'00' if undetermined, appears in the fourth byte of the sense data.

Sense code 200A

Immediate request mode error: The immediate request mode protocol has been violated by the request.

Sense code 200B

Queued response error: The queued response protocol has been violated by a request; that is, QRI=¬QR when an outstanding request had QRI=QR.

Sense code 200C

ERP sync event error: The ERP sync event protocol in DFC has been violated; for example, after receiving a negative response to a chain, a request other than a request soliciting a synchronization event response was sent to DFC_SEND and rejected.

Sense code 200D

Response owed before sending request: An attempt has been made in half-duplex (flip-flop or contention) send/receive mode to send a normal-flow request when a response to a previously received request has not yet been sent.

Sense code 200E

Response correlation error: A response was received that cannot be correlated to a previously sent request.

Sense code 200F

Response protocol error: A violation has occurred in the response protocol; for example, a +RSP to an RQE chain was generated.

Sense code 2010

BIS protocol error: A BIS protocol error was detected; for example, a BIS request was received after a previous BIS was received and processed.

Sense code 2011

Pacing protocol error.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
A normal-flow request was received by a half-session after the pacing count had been reduced to zero and before a pacing response had been sent.

0001
Unexpected isolated pacing message (IPM) received: An IPM was received when the receiver was in a state that did not allow it.

0002
Unexpected pacing request received: A request with the pacing indicator set was received when the receiver was in a state that did not allow it.

0003
Pacing response indicator incorrectly set: The pacing indicator was set in a non-IPM response received while adaptive pacing was being used.

Sense code 2012

Sense code received not valid: A negative response was received that contains an SNA-defined sense code that cannot be used for the sent request.

Sense code 2013

Decompression protocol error: A request containing compressed data was received in error.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The decompressor received a compressed RU without an expected reset decompression control sequence. The compressor and the decompressor are not synchronized.

0002
The decompressor received a compressed RU containing a decompression control sequence that is not valid. The compressor and the decompressor are not synchronized.

0003
The length of the decompressed RU did not match the length given in the compression header.

0004
The decompressor has determined that the compression header indicates an illegal compression algorithm was used. The compression algorithm was not agreed to during the session-activation negotiation.

0005
The decompressor has detected that the decompressed RU size exceeds the maximum RU size.

40XX (RH usage error)

This category indicates that the value of a field or combination of fields in the RH violates architectural rules or previously selected BIND options. These errors prevent delivery of the request to the intended component and are independent of the current states of the session. They might result from the failure of the sender to enforce session rules. Detection by the receiver of each of these errors is optional.

Category and modifier (in hexadecimal):

4001
SC or NC RH not valid: The RH of a session control (SC) or network control (NC) request was not valid. For example, an SC RH with pacing request indicator set to one is not valid.

4003
BB not allowed: The begin bracket indicator (BBI) was specified incorrectly, for example, BBI=BB with BCI=¬BC.

4004
CEB or EB not allowed: The conditional end bracket indicator (CEBI) or end bracket indicator (EBI) was specified incorrectly, for example, CEBI=CEB when ECI=¬EC or EBI=EB with BCI=¬BC, or by the primary half-session when only the secondary may send EB, or by the secondary when only the primary may send EB.

4005
Incomplete RH: Transmission shorter than full TH-RH.

4006
Exception response not allowed: Exception response was requested when not permitted.

4007
Definite response not allowed: Definite response was requested when not permitted.

4008
Pacing not supported: The pacing indicator was set on a request, but the receiving half-session or boundary function half-session does not support pacing for this session.

4009
CD not allowed: The change direction indicator (CDI) was specified incorrectly, for example, CDI=CD with ECI=¬EC, or CDI=CD with EBI=EB.

400A
No-response not allowed: No-response was specified on a request when not permitted. (Used only on EXR.)

400B
Chaining not supported: The chaining indicators (BCI and ECI) were specified incorrectly, for example, chaining bits indicated other than (BC,EC), but multiple-request chains are not supported for the session or for the category specified in the request header.

400C
Brackets not supported: The bracket indicators (BBI, CEBI, and EBI) were specified incorrectly, for example, a bracket indicator was set (BBI=BB, CEBI=CEB, or EBI=EB), but brackets are not used for the session.

400D
CD not supported: The change-direction indicator was set, but is not supported.

400F
Incorrect use of format indicator: The format indicator (FI) was specified incorrectly, for example, FI was set with BCI=¬BC, or FI was not set on a DFC request.

4010
Alternate code not supported: The code selection indicator (CSI) was set when not supported for the session.

4011
Incorrect specification of RU category: The RU Category indicator was specified incorrectly, for example, an expedited-flow request or response was specified with RU Category indicator = FMD.

4012
Incorrect specification of request code: The request code on a response does not match the request code on its corresponding request.

4013
Incorrect specification of (SDI, RTI): The sense data included indicator (SDI) and the response type indicator (RTI) were not specified properly on a response. The proper value pairs are (SDI=SD, RTI=negative) and (SDI=¬SD, RTI=positive).

4014
Incorrect use of (DR1I, DR2I, ERI): The definite response 1 indicator (DR1I), definite response 2 indicator (DR2I), and exception response indicator (ERI) were specified incorrectly, for example, a SIGNAL request was not specified with DR1I=DR1, DR2I=¬DR2, and ERI=¬ER.

4015
Incorrect use of QRI: The queued response indicator (QRI) was specified incorrectly, for example, QRI=QR on an expedited-flow request.

4016
Incorrect use of EDI: The enciphered data indicator (EDI) was specified incorrectly, for example, EDI=ED on a DFC request.

4017
Incorrect use of PDI: The padded data indicator (PDI) was specified incorrectly, for example, PDI=PD on a DFC request.

4018
Incorrect setting of QRI with bidder's BB: The first speaker half-session received a BB chain requesting use of a session [via LUSTAT(X'0006')], but the QRI was specified incorrectly; that is, QRI=¬QR.

4019
Incorrect indicators with last-in-chain request: A last-in-chain request has specified incompatible RH settings, for example, RQE*, CEBI=¬CEB, and CDI=¬CD.

4021
QRI setting in response different from that in request: The QRI setting in the response differs from the QRI setting in the corresponding request.

80XX (path error)

This category indicates that the request could not be delivered to the intended receiver, because of a path outage, a sequence of activation requests that is not valid, or one of the listed path information unit (PIU) errors. Some PIU errors fall into other categories; for example, sequence number errors are sense code category X'20'. A path error received while the session is active generally indicates that the path to the session partner has been lost.

Category and modifier (in hexadecimal):

Sense code 8000

A path error occurred, but no further information about the error is available. Errors occurred because of an outstanding I/O request being purged. For example, an ACB for an application which has outstanding I/O requests received INOP, or an operator entered VARY INACT for resources that had outstanding I/O requests.

VTAM hint: If you receive this code when attempting to send data over an active Enterprise Extender PU, ensure that UDP ports 12001 and 12004 on all firewalls in the path of the IP traffic are open and allowing the traffic through.

Sense code 8001

Intermediate node failure: Machine or program check in a node providing intermediate routing function. A response might or might not be possible.

Sense code 8002

Link failure: Data link failure.

0000
No specific code applies.

VTAM hints:

- If the IST1097I message group is displayed with this sense code, followed by a display of the IST1110I message group with sense code X'80140001', then the CP-CP session failed due to the loss of the last CP-capable connection with the adjacent control point.
- If 80020000 received for session using a switched PU that has DISCNT=YES and is in the process of inactivating because there are no more LU-LU sessions, this is a temporary condition and the session might be tried again.
- If 80020000 received for session using a switched PU that is receiving simultaneous inbound and outbound calls, this is a temporary condition and the session might be tried again.

Sense code 8003

NAU inoperative: The NAU is unable to process requests or responses; for example, the NAU has been disrupted by an abnormal termination.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

VTAM hint: A possible cause of this error is that the LU is inoperative.

0001
Hierarchical reset: The identified LU-LU session is being deactivated; an ACTLU/ACTPU (Cold) or DACTLU/DACTPU was received, or the PU has failed.

0003
Unrecoverable LU failure: The identified LU-LU session had to be deactivated because of an abnormal termination of the PLU or SLU; recovery from the failure was not possible.

0004
Recoverable LU failure: The identified LU-LU session had to be deactivated because of an abnormal termination of one of the LUs of the session; recovery from the failure might be possible.

0005
Hierarchical reset: Backup session reset resulted from a hierarchical reset.

Sense code 8004

Unrecognized destination: A node in the path has no routing information for the destination specified either by the SLU name in a BIND request or by the TH.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- The destination address field (DAF) is not recognized.
- There might be a hardware problem with the PU.

0001
A request received by a gateway function could not be rerouted because of routing information that is incomplete or not valid.

Sense code 8005

No session: No half-session is active in the receiving end node for the indicated origination-destination pair, or no boundary function session connector is active for the origin-destination pair in a node providing the boundary function. A session activation request is needed.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

VTAM hint: If this sense code is displayed in message IST1280I, take one of the following actions:

- Perform an operator activation of the CP-CP session by entering a VARY ACT,ID=*adjcpname* command at the end node.
- Modify the network node server list to include either an explicit entry for the desired network node or a nameless entry.

0001
The receiver received a request other than a session control request when no LU-LU session was active.

0002
The receiver received a request other than a session control request when no LU-SSCP session was active.

0003
The receiver received a session control request other than BIND/UNBIND when no LU-LU session was active.

0004
The receiver received an UNBIND when no LU-LU session was active.

0005
The receiver received a session control request other than ACTLU/DACTLU for the LU-SSCP session when no LU-SSCP session was active.

0006
The receiver received DACTLU when no LU-SSCP session was active.

0007
Session not activated: A BIND was received for a dependent LU that has not received an ACTLU to activate the SSCP-LU session.

0008
A request could not be forwarded to the destination node because an active session with that node did not exist. The name of the node that could not forward the request is indicated in the accompanying name list (X'06') subvector.

Sense code 8006

FID not valid: FID is not valid for the receiving node.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The FID-5 transmission header (TH) that was received contained errors that precluded further processing of the message.

Sense code 8007

Segmenting error: First BIU segment had fewer than ten bytes; or mapping-field sequencing error, such as first, last, middle; or segmenting not supported and mapping field not set to BBIU, EBIU.

Note: If segmenting is not supported, a negative response is returned for the first segment only because this contains the RH. Subsequent segments are discarded.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The node does not support receipt of segments, and a mapping field value other than BBIU, EBIU was received. Sent in UNBIND.

0002
Interleaved BIND segments not allowed: A BIND receiver that is in the middle of receiving segments of one BIND receives a segment from a different BIND; the receiver rejects both BINDs and disconnects all the links in the transmission group.

Sense code 8008

PU not active: The SSCP-PU secondary half-session in the receiving node has not been activated, and the request was not ACTPU for this half-session; for example, the request was ACTLU from an SSCP that does not have an active SSCP-PU session with the PU associated with the addressed LU.

Bytes 2 and 3 following the sense code contain sense code specific information.

0001
A physical unit name was specified for an independent LU session tail. The specified PU is either unknown or in a state that is not valid.

0002
No ALS (adjacent link station) list was provided for an independent LU. You must define an ALS for an independent LU if you want to use VARY LOGON and LOGAPPL for the independent LU. You can also use VTAM functions to dynamically determine an ALS.

Sense code 8009

LU not active: The destination address specifies an LU for which the SSCP-LU secondary half-session has not been activated and the request was not ACTLU.

Sense code 800A

Too-long PIU: Transmission was truncated by a receiving node because the PIU exceeded a maximum length or sufficient buffering was not available.

VTAM hint: A possible cause of this error is that a session ended unexpectedly and either no message is received or an exception request (EXR) is generated with this sense code. When an application receives an exception request or response with this sense code, it usually ends the session. No VTAM message is

issued, but the application might issue a message. This can occur when a path information unit (PIU) is too large to be passed from one node to another. See the information about common subarea network problems in the z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information about this problem or see APAR II03990.

Sense code 800B

Incomplete TH: Transmission received was shorter than a TH.

Note: It is generally not possible to send a response for this exception condition, because the information (FID, addresses) that is required to generate a response is not available.

Sense code 800C

DCF error: Data count field inconsistent with transmission length.

Sense code 800D

Lost contact: Contact with the link station for which the transmission was intended has been lost, but the link has not failed. If the difference between link failure and loss of contact is not detectable, link failure (X'8002') is sent.

Sense code 800E

Unrecognized origin: The origin address specified in the TH was not recognized.

Sense code 800F

The address combination is not valid.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
The (DAF',OAF') (FID2) combination or the LSID (FID3) specified a type of session that is not valid, for example, a PU-LU combination.

0001
The FID2 ODAI setting in a received BIND is incorrect; the BIND is rejected.

Sense code 8010

Segmented RU length error: An RU was found to exceed a maximum length, or required buffer allocation that might cause future buffer depletion.

Sense code 8011

ER inoperative or undefined: A PIU was received from a subarea node that does not support ER and VR protocols, and the explicit route to the destination is inoperative or undefined.

Sense code 8012

Subarea PU not active, or invalid virtual route: A session-activation request for a peripheral PU or LU cannot be satisfied because there is no active SSCP-PU session for the subarea node providing boundary function support, or the virtual route for the specified SSCP-PU (Type 1 or Type 2 nodes) or SSCP-LU session is not the same as that used for the SSCP-PU session of the Type 1 or Type 2 node's PU or the LU's subarea PU.

Sense code 8013

Route not available: No route is available to connect the specified origin subarea (OSA) and destination subarea (DSA) for the specified COS.

Note: If none of the virtual routes specified in the VR identifier list or route specification for the session is active or can be activated, the reported reason is set based on a hierarchy of failure events. The "highest" of the failures that occurred within the set of virtual routes is returned on the response. For example, if the VR manager receives a negative response to an NC_ACTVR request for a VR specified in the VR identifier list and for all other VRs in the list no VR to ER mapping is specified, reason X'nn06' is reported. The hierarchy of the failure reasons is in ascending numeric order; that is, reason X'nn02' is higher than reason X'nn01'.

Bytes 2 and 3 following the sense code indicate the environment in which the failure was detected and the reason for the failure.

0000
No specific code applies: This means an error occurred, but none of the conditions listed below applies. This code is issued in a single network environment.

VTAM hint: Possible causes for this error include, but are not limited to, the following ones:

- The subarea class of service is not known. Verify that the node issuing the sense code has a usable subarea class of service for the mode associated with the session request. This problem can occur when a mode table is copied from one node to another, and the subarea classes of service specified by the table no longer map to valid COS names defined at that node.
- There is an error in the path definitions.

0001
No mapping specified: A session-activation request cannot be satisfied because for each VR in the VR identifier list for the session, no VR to ER mapping is specified.

0002
No explicit routes defined: A session-activation request cannot be satisfied because each VR in the VR identifier list for the session maps to a corresponding ER that is not defined. This code is issued in a single network environment.

0003
No VR resource available: A session-activation request cannot be satisfied because each VR specified in the VR identifier list for the session requires a node resource that is not available. This code is issued in a single network environment.

0004
No explicit routes operative: A session-activation request cannot be satisfied because no underlying ER is operative for any VR specified in the VR identifier list for the session. This code is issued in a single network environment.

0005
No explicit route can be activated: A session-activation request cannot be satisfied because no VR specified in the VR identifier list for the session mapped to a defined and operative ER that could be activated. This code is issued in a single network environment.

0006
No virtual route can be activated: A session-activation request cannot be satisfied because no VR specified in the VR identifier list for the session can be activated by the PU, though, for at least one VR, an underlying ER is defined, operative, and activated. This code is issued in a single network environment.

0007
No virtual route identifier list available: A session-activation request cannot be satisfied because a route specification is unavailable or incomplete. A valid route specification is either a VR identifier list or a route dynamics route specification control vector. This code is issued in a single network environment.

0100
No specific code applies: This means an error occurred, but none of the conditions listed below applies. This code is issued in an interconnected network. The failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

0101
No mapping specified: A session-activation request cannot be satisfied because for each VR in the VR identifier list for the session, no VR to ER mapping is specified. This code is issued in an interconnected network. The failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

VTAM hint: Ensure that the PATH definition statement for the gateway NCP contains VRs coded for the networks in both directions.

0102
No explicit routes defined: A session-activation request cannot be satisfied because each VR in the VR identifier list for the session maps to a corresponding ER that is not defined. This code is issued in an interconnected network. The failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

0103
No VR resource available: A session-activation request cannot be satisfied because each VR specified in the VR identifier list for the session requires a node resource that is not available. This code is issued in an interconnected network. The failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

0104
No explicit routes operative: A session-activation request cannot be satisfied because no underlying ER is operative for any VR specified in the VR identifier list for the session. This code is issued in an interconnected network. The failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

0105
No explicit route can be activated: A session-activation request cannot be satisfied because no VR specified in the VR identifier list for the session mapped to a defined and operative ER that could be activated. This code is issued in an interconnected network. The failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

0106
No virtual route can be activated: A session-activation request cannot be satisfied because no VR specified in the VR identifier list for the session can be activated by the PU, though, for at least one VR, an underlying ER is defined, operative, and activated. This code is issued in an interconnected network. The failure was detected at a node in a subnetwork other than that of the NAU sending the activation request.

0107
No virtual route identifier list available: A session-activation request cannot be satisfied because a route specification is unavailable or incomplete. A valid route specification is either a VR identifier list or a route dynamics route specification control vector.

Sense code 8014

No path exists to the destination node: Route selection services in the CP has determined from the topology database that no path exists to the destination node.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
No route to the destination node exists for the specified class of service.

VTAM hint: Possible causes of this error include, but are not limited to, the following ones:

- If the IST1097I message group is displayed with the X'80020000' sense code, followed by a display of the IST1110I message group with this sense code, then the CP-CP session failed due to the loss of the last CP-capable connection with the adjacent control point.

- If there are multiple entry points to the subarea network, there must be a COS-acceptable route from the origin node to each interchange node that represents a possible subarea entry point to be used to reach the destination LU. A COS-acceptable route is a route that is acceptable for the class of service specified on the session request.

  Examine your network configuration to determine if a valid path does exist. Use the DISPLAY TOPO command to verify that the topology database currently shows the links in the path as operational. If a valid APPN path exists, the characteristics of the nodes and links in the operational paths might not meet the requirements of the specified class of service. Do the following checks:

  – Verify that the mode name specified on the request maps to the intended class of service.
  – Examine the LINEROWs and NODEROWs in the class of service definition to determine what the allowable ranges are for the link and node characteristics.
  – Use the DISPLAY TOPO command to view the characteristics of the nodes and TGs in the likely paths. Look for the following problems:
    - Nodes in the path are congested or have route resistance values outside the limits set by the class of service.
    - The COS definition required secure links, but no path exists consisting exclusively of secure TGs.
    - High capacity (speed) was required by the COS definition, but no path exists in which all of the links are fast enough to meet the specified minimum capacity.
- When one of the session partners resides on an end node (EN) that has many links (TGs) to other nodes, this sense code might be set by the network node (NN) responsible for computing the session path if that NN did not receive a complete list of the EN's active links (TG vectors). This can happen when some of the EN TG Vectors are removed from the APPN Locate search because including all of them would result in an APPN Locate search that exceeds the maximum APPN Locate size supported by every node along the APPN Locate search path. See Maximum APPN Locate Size Considerations in z/OS Communications Server: SNA Network Implementation Guide for more information.

0002
COS name received is not valid.

VTAM hint: The most common reasons for this error are:

- The requested APPN class-of-service (COS) definition is not found in the COS database at the node issuing this sense code.
- The requested mode name for the session does not map to an APPN class of service known by this node.

Examine the mode definition to determine the APPN COS name. Verify that this definition exists in a VTAMLST member at the nodes which resolve the mode to an APPN class of service. Activate the member to ensure that the definition is active. If APPN COS substitution has been enabled by specifying the APPNCOS start option, verify that the COS it specifies has been activated.

0003
The topology database indicates that the destination node is not available at this time; the node either has inconsistent data or is quiescing.

VTAM hint: This sense code might be issued when an attempt is made to change the node role of the destination node of a TG that is being activated and the node role change fails.

0004
The topology database indicates that the endpoint resources are depleted; the node is out of either half-session control blocks or message buffers.

0005
The length of the generated RSCV exceeds the maximum allowed.

VTAM hint: This sense code indicates that the attempt to build the route selection control vector failed because the number of hops between the origin and destination nodes was too large.

Examine your network configuration to determine how many hops would be expected in the best route for the requested APPN class of service. If the number of hops within a single APPN subnetwork is greater than six, you might need to provide a more direct origin-to-destination path.

If you are using connection network routing, reducing the length of the connection network name reduces the length of the generated RSCV. The reduced RSCV might be shorter than the maximum length allowed.

If you are using hostname resolution for Enterprise Extender connection network processing, reducing the length of the hostnames passed to name-to-address resolution reduces the length of the generated RSCV. The reduced RSCV might be shorter than the maximum length allowed.

0006
No path using only HPR (high-performance routing) links exists to the destination node.

0007
BIND RSCV consists of only an interchange TG.

VTAM hint: An RSCV was calculated that consisted of only interchange TGs. APPN Locates will not be used to set up the session.

0008
This node calculated an RSCV in which it does not own the boundary function.

VTAM hint: This node calculated an RSCV in which it doesn't own the boundary function.

Sense code 8015

Path not available.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0004
The internetwork locate failed because an internetwork route did not exist that matched the requested class of service.

VTAM hint: An error has occurred during COS mapping in a node supporting APPN multiple network connectivity. Whenever a search crosses an APPN subnetwork link, the node receiving the search must map the COS it received to an equivalent COS to be used in its subnet. The COS being mapped is defined by the user in the COSMAP definition deck. The error occurs when the user maps the original COS to a COS that has not been defined within this node.

Sense code 8016

Not a proper ER.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000
No specific code applies.

0001
The ER is not in the proper state for routing a PIU, as indicated by the state of the dynamic routing table entry.

Sense code 8017

PIU from adjacent pre-ER-VR subarea node rejected: A PIU that requires intermediate path-control routing was received by a subarea node from an adjacent subarea node that does not support ER-VR protocols, but the receiving subarea node does not support intermediate path-control routing for adjacent subarea nodes that do not support ER-VR protocols.

Sense code 8018

Management services component is unable to find or recognize the name of the application transaction program specified in the request.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

Operations management is unable to route the MDS_MU to the served application specified in the DAN field of the R and TI because the served application's subtask is not active.

0001
The application transaction program specified in the request is not recognized by physical unit management services (PUMS).

Sense code 8019

Routing exception: a node is unable to perform the required routing function for a request.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
Unknown routing group name.

0002
Unknown routing group name, routing element name combination.

0004
No connection is available for level of service required.

0005
The routing and targeting instructions GDS variable is is required but is not present.

0006
The internetwork route selection subfield (IRSS) was required to be included in a BIND RSCV, but was either missing or had a format which was not valid.

0007
The internetwork route selection subfield (IRSS) was required to be included in a locate request or reply, but was either missing or had format that was not valid.

0008
The border node detected multiple instances of its own name in the internetwork route selection subfield (IRSS) in a locate request or reply or in a BIND, indicating a routing loop.

0009
An explicit route was not available to permit activation of a virtual route-based APPN TG.

000A
An activation request was received that was not valid for the current state of the specified virtual route-based APPN TG.

000B
Origin node not found. TRS received a route calculation request with no origin endpoint TG vectors and could not find a node entry for the origin node in the topology database.

000C
When the DLUS node received a locate request for a DLUS-served dependent LU, the DLUS node determined that at least one intersubnetwork TG on the path between DLUS and the PLU was not between two extended border nodes.

VTAM hint: The dependent LU server (DLUS) and the PLU node are in different APPN subnetworks, which requires that an extended border node be present in both the PLU subnetwork and the DLUS

subnetwork. This session path does not have an extended border node in either the PLU subnetwork or the DLUS subnetwork.

Sense code 801C

Hop count exhausted.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
The request has been forwarded by an excessive number of nodes (for example, the count has been decremented at each node and has reached zero) and, therefore, the request could not be delivered to one or more destinations. Typically, this exception indicates that one or more nodes have incorrectly routed or directed the request. The exception might also indicate that the routing/directing count was not appropriately initiated according to network size.

Sense code 8020

Session reset: The LU-LU session identified in the UNBIND is being deactivated because of a reset condition.

Bytes 2 and 3 following the sense code contain sense code specific information.

0000
No specific code applies.

0001
Virtual route inoperative: The virtual route used by the LU-LU session has become inoperative, thus forcing the deactivation of the identified LU-LU session.

0002
Hierarchical reset of both XRF-active and XRF-backup sessions: The XRF-backup session has failed; therefore, both the XRF-active and XRF-backup session are being reset.

0003
Virtual route deactivated: The identified LU-LU session had to be deactivated because of a forced deactivation of the virtual route being used by the LU-LU session.

0004
Route extension failure: The route extension used by the LU-LU session has become inoperative, thus forcing the deactivation of the identified LU-LU session.

0005
Route extension failure: The route extension used by the XRF-backup LU-LU session has become inoperative, thus forcing the deactivation of the identified XRF-backup LU-LU session.

0006
Virtual route inoperative: The virtual route used by the LU-LU session has become inoperative, thus forcing the deactivation via VR-INOP of the identified XRF-backup LU-LU session.

0007
An LU requested termination.

0008
BFTERM has been received with no indication of the cause of the reset.

0009
Termination was requested by the dependent SLU with a TERMINATE_SELF or character coded LOGOFF.

000A
The identified LU-LU session had to be deactivated because its underlying RTP connection has become inoperative.

000B
The identified LU-LU session had to be deactivated because its underlying RTP connection was deactivated.

000D
The cross-domain resource session has been terminated.

Sense code 8021

Path switch failure: The attempt to switch the path traversed by an RTP connection has failed.

Bytes 2 and 3 following the sense code contain sense code specific information. Settings allowed are:

0000
No specific code applies.

0001
The original path of the RTP connection is inoperative. Because the path switch failed, all sessions using the RTP connection will be terminated.

0002
The original path of the RTP connection is still operative. The RTP connection will continue operation over the original path.

A0XX (RTP sense data)

This category generally indicates that an RTP machine detects a protocol violation and terminates the RTP connection. The A002 category of sense codes does not indicate that a protocol violation has been detected.

Category and modifier (in hexadecimal):

Sense code A001

The RTP connection failed.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0003
The setting of the start-of-message bit in a received packet was unexpected. One of the following error conditions was detected:

- During reassembly of a user message, the byte-sequence-number field of a received packet is set to the next expected sequence number of the user message, but the start-of-message bit is set to one.
- The byte-sequence-number field of a received packet containing data is set to the expected starting sequence number of a user message, but the start-of-message bit is set to zero.
- The byte-sequence-number field of a received packet is set to the expected starting sequence number of a user message. The end-of-message bit is set to one, but the start-of-message bit is set to zero.
- Lower sequence-numbered data was received in an earlier packet with the last-message bit set to one, but the start-of-message bit is set to one in the newly received packet.

0004
The setting of the end-of-message (EOMI) bit in a received packet was unexpected. One of the following error conditions was detected:

- A packet containing data has the last-message bit (LMI) set to one, but the end-of-message bit is set to zero.
- During reassembly of a user message, the byte-sequence-number field of a received packet is set to the next expected sequence number of the user message; the last-message bit is set to one, but the end-of-message bit is set to zero.

- The byte-sequence-number field of a received packet is set to the expected starting sequence number of a user message. The start-of-message bit (SOMI) is set to one, the last-message bit is set to one, but the end-of-message bit is set to zero.

0008
The setting of the last-message bit in a received packet was unexpected. The following error condition was detected:

The last-message bit is set to one in a retransmitted packet, but higher sequence-numbered data was received in an earlier packet.

000B
The setting of the "connection qualifier source identifier field present" bits in a received packet was unexpected. The following error condition was detected:

The TCID-assignor bit is set to one, but the "connection qualifier/source identifier field present" bits are not set to 01.

000C
The setting of the "optional segments present" bit in a received packet was unexpected. The following error condition was detected:

No active context is found, the setup-packet bit is set to one, but the "optional segments present" bit is set to zero.

000D
The setting of the DATA OFFSET/4 in the THDR field in a received packet was unexpected. One of the following error conditions was detected:

- The data-length field has a value greater than zero, but the payload-offset/4 field points to an offset beyond the end of the network layer packet.
- The data-length field has a value greater than zero, but the setting of the DATA OFFSET/4 field is not consistent with the encodings of the connection-qualifier/source-identifier field and the optional segments.

000E
The setting of the DATA length field in the THDR of a received packet was unexpected. One of the following error conditions was detected:

- The data-length field has a value greater than zero, but the DATA OFFSET/4 field points to an offset from which there is insufficient remaining length for the data.
- The packet contains data, but lower sequence-numbered data was received in an earlier packet with the last-message bit set to one.

000F
The setting of the byte sequence number field (BSN) in a received packet was unexpected. The following error condition was detected:

The byte-sequence-number field of a received packet is higher than the next expected sequence number (that is, a new gap in the user data stream is detected), but the last-message bit was set to one in an earlier packet.

0014
The setting of the target resource identifier field present bit of the connection setup segment in a received packet was unexpected. The following error condition was detected:

The target resource identifier field present bit in the connection setup segment is set to zero, but target resource identification is required by the receiver.

0016
The setting of the ARB flow congestion control used bit of the connection setup segment in a received packet was unexpected. The following error condition was detected:

The ARB flow/congestion control used bit is set to zero, but the use of ARB flow/congestion control is required by the receiving RTP.

0017
A field setting in the topic identifier (X'28') control vector in the connection setup segment in a received packet was unexpected. One of the following error conditions was detected:

- The topic-identifier field within the topic-identifier (X'28') control vector is not correctly encoded.
- The topic identifier specified in the topic-identifier (X'28') control vector is not supported.

0018
A field setting in the network identifier (X'03') control vector in a received packet was unexpected. One of the following error conditions was detected:

- The network-identifier field within the network-identifier (X'03') control vector is not correctly encoded.
- The network-identifier specified in the network-identifier (X'03') control vector within the connection-setup segment is not the network identifier associated with the receiving RTP.

0019
A field setting in the node identifier (X'00') control vector in a received packet was unexpected. One of the following error conditions was detected:

- The node-identifier field within the node-identifier (X'00') control vector is not correctly encoded.
- The node-identifier specified in the node-identifier (X'00') control vector within the connection-setup segment is not the node identifier associated with the receiving RTP.

001E
The setting of the closed bit of the status segment in a received packet was unexpected. One of the following error conditions was detected:

- The closed bit in the status segment is set to one, but not all reliable data sent to the partner is acknowledged.
- The closed bit in the status segment is set to one, but data is queued for transmission.

001F
The setting of the ARB level in the ARB segment in a received packet was unexpected. The following error condition was detected:

- Progressive-mode ARB is specified in the ARB segment, but it is not allowed on this connection.

0022
The setting of the DSEQ field of the status segment in a received packet was unexpected. The following error condition was detected:

RSEQ and DSEQ in the status segment are not consistent. The values indicate data not received has been delivered.

0032
The beginning and ending sequence numbers for an acknowledged byte-span pair (ABSP) in a status segment in a received packet were unexpected. The following error condition was detected:

The beginning and ending sequence numbers for an ABSP are not consistent either with RSEQ or another ABSP. The sequence numbers overlap.

0033
A field setting in the HPR switching information (X'83') control vector in a received packet was unexpected. The following error condition was detected:

The maximum packet size specified in the HPR switching information (X'83') control vector is fewer than 768 bytes.

0035
A field setting in the NCE identifier (X'26') control vector in a received packet was unexpected. The following error condition was detected:

The NCE-identifier field within the NCE-identifier (X'26') control vector is not correctly encoded.

0037
Window flow control was requested by the calling RTP but is not supported by the listening RTP.

003A
The using layer terminated abnormally. (This error condition is associated with the RTP user interface and is implementation dependent.)

Sense code A002

The RTP connection is terminating.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0001
The sense code sent a connection fault to inform the RTP partner that this end of the pipe is terminating. The RTP partner should not treat this as an error case, but rather terminate its endpoint without issuing an alert. This flow might occur, after a failure to path switch, as a final effort to notify the RTP partner that the pipe is being terminated. The partner RTP should clean up its end of the connection upon receipt of the connection fault.

Sense code A018

The RTP connection failed.

0000
An RTP control vector length error was detected. The value in the length field of the control vector added to the current byte offset within the embedding structure (either an optional segment or control vector) exceeds the actual length of the embedding structure, or the value in the length field is inconsistent with the format definition for the control vector. nn is the key of the control vector in error. mm is the key of the embedding control vector or optional segment. One of the following error conditions was detected:

- The length of the node identifier (X'00') control vector exceeds the remaining length of the network address (X'05') control vector, or the length of the node identifier control vector is inconsistent with its format definition — X'A0180500'.
- The length of the network identifier (X'03') control vector exceeds the remaining length of the network address (X'05') control vector, or the length of the network identifier control vector is inconsistent with its format definition — X'A0180503'.
- The length of the NCE identifier (X'26') control vector exceeds the remaining length of the network address (X'05') control vector, or the length of the NCE identifier control vector is inconsistent with its format definition — X'A0180526'.
- The length of an unrecognized control vector contained within the network address (X'05') control vector exceeds the remaining length of the network address control vector — X'A01805xx', where xx is the key of the unrecognized control vector.
- The length of the node identifier (X'00') control vector exceeds the remaining length of the connection setup segment, or the length of the control vector is inconsistent with its format definition — X'A0180D00'.
- The length of the network identifier (X'03') control vector exceeds the remaining length of the connection setup segment, or the length of the control vector is inconsistent with its format definition — X'A0180D03'.
- The length of the topic identifier (X'28') control vector exceeds the remaining length of the connection setup segment, or the length of the control vector is inconsistent with its format definition — X'A0180D28'.
- The length of the HPR switching information (X'83') control vector exceeds the remaining length of the switching information segment, or the length of the control vector is inconsistent with its format definition — X'A0181483'.
- The length of return ANR field specified in the HPR switching information (X'83') control vector is greater than the remaining length of the control vector — X'A0181483'.

- The length of the HPR return route TG descriptor (X'85') control vector exceeds the remaining length of the switching information segment, or the length of the control vector is inconsistent with its format definition — X'A0181485'.

FF00
An RTP optional segment or control vector length error was detected. The value in the length field of the optional segment or control vector added to the current byte offset within the embedding structure, the RTP transport header, exceeds the actual length of the embedding structure, or the value in the length field is inconsistent with the format definition for the optional segment or control vector. 00 is the key of the optional segment or control vector in error. One of the following error conditions was detected:

- The length of the network address (X'05') control vector exceeds the remaining length of the network layer packet — X'A018FF05'.
- The length of the connection setup segment exceeds the remaining length of the network layer packet, or the length of the segment is shorter than its minimum length — X'A018FF0D'.
- The length of the status segment exceeds the remaining length of the network layer packet, or the length of the segment is shorter than its minimum length — X'A018FF0E'.
- The number of acknowledged byte span pairs specified in the status segment is inconsistent with the length of the segment — X'A018FF0E'.
- The length of the client out-of-band bits segment exceeds the remaining length of the network layer packet, or the length of the segment is shorter than its minimum length — X'A018FF0F'.
- The length of the connection identifier exchange segment exceeds the remaining length of the network layer packet, or the length of the segment is shorter than its minimum length — X'A018FF10'.
- The length of the connection fault segment exceeds the remaining length of the network layer packet, or the length of the segment is shorter than its minimum length (no connection fault segment is returned to the partner) — X'A018FF12'.
- The length of the switching information segment exceeds the remaining length of the network layer packet, or the length of the segment is shorter than its minimum length — X'A018FF14'.
- The length of the adaptive rate-based segment exceeds the remaining length of the network layer packet, or the length of the segment is shorter than its minimum length — X'A018FF22'.
- The length of an unrecognized optional segment exceeds the remaining length of the network layer packet — X'A018FFxx', where xx is the key of the unrecognized optional segment.

Sense code A019

The RTP connection failed.

FF00
RTP received an optional segment or control vector embedded within the RTP transport header, but the optional segment or control vector is not valid in the current state of the connection. 00 is the key of the unexpected optional segment or control vector. The following error condition was detected:

The packet was received from the listening partner, but it contained a Connection Setup segment — X'A019FF0D'.

Sense code A01A

The RTP connection failed.

FF00
RTP received two or more control vectors or optional segments with the same key embedded within the RTP transport header. The number of occurrences of the control vector or optional segment is more than is valid for the current state of the connection. 00 is the key of the duplicated optional segment or control vector. One of the following error conditions was detected:

- The packet contained multiple connection setup segments — X'A01AFF0D'.

- The packet contained multiple status segments — X'A01AFF0E'.
- The packet contained multiple client out-of-band bits segments — X'A01AFF0F'.
- The packet contained multiple connection identifier exchange segments — X'A01AFF10'.
- The packet contained multiple switching information segments — X'A01AFF14'.
- The packet contained multiple adaptive rate-based segments — X'A01AFF22'.

FF80
RTP received two or more control vectors or optional segments with the same key embedded within the RTP transport header. The number of occurrences of the control vector or optional segment is more than is valid for the current state of the connection. 80 is the key of the duplicated optional segment or control vector. One of the following error conditions was detected:

- The packet contained multiple connection setup segments — X'A01AFF0D'.
- The packet contained multiple status segments — X'A01AFF0E'.
- The packet contained multiple client out-of-band bits segments — X'A01AFF0F'.
- The packet contained multiple connection identifier exchange segments — X'A01AFF10'.
- The packet contained multiple switching information segments — X'A01AFF14'.
- The packet contained multiple adaptive rate-based segments — X'A01AFF22'.

Sense code A01B

The RTP connection failed.

0000
RTP received an optional segment or control vector that did not contain a required control vector. 00 is the key of the missing control vector. 00 is the key of the embedding control vector or optional segment. One of the following error conditions was detected:

- The network address (X'05') control vector does not contain a node identifier (X'00') control vector — X'A01B0500'.
- The network address (X'05') control vector does not contain a network identifier (X'03') control vector — X'A01B0503'.
- The network address (X'05') control vector does not contain an NCE identifier (X'26') control vector — X'A01B0526'.

0500
RTP received an optional segment or control vector that did not contain a required control vector. 00 is the key of the missing control vector. 05 is the key of the embedding control vector or optional segment. The following error condition was detected:

The network address (X'05') control vector does not contain a node identifier (X'00') control vector — X'A01B0500'.

0503
RTP received an optional segment or control vector that did not contain a required control vector. 03 is the key of the missing control vector. 05 is the key of the embedding control vector or optional segment. The following error condition was detected:

The network address (X'05') control vector does not contain a network identifier (X'03') control vector — X'A01B0503'.

0526
RTP received an optional segment or control vector that did not contain a required control vector. 26 is the key of the missing control vector. 05 is the key of the embedding control vector or optional segment. The following error condition was detected:

The network address (X'05') control vector does not contain an NCE identifier (X'26') control vector — X'A01B0526'.

FF00
RTP received a packet in which the RTP transport header did not contain a required optional segment or control vector. 00 is the key of the missing optional segment or control vector. One of the following error conditions was detected:

- The TCID assignor bit is set to one, the connection qualifier/source identifier field present bits are set to 01, but no network address (X'05') control vector is present — X'A01BFF05'.
- No active context is found, the setup packet bit is set to one, but no connection setup segment is found — X'A01BFF0D'.

FF05
RTP received a packet in which the RTP transport header did not contain a required optional segment or control vector. *nn* is the key of the missing optional segment or control vector. One of the following error conditions was detected:

- The TCID Assignor bit is set to one, the connection qualifier/source identifier field present bits are set to 01, but no network address (X'05') control vector is present — X'A01BFF05'.
- No active context is found, the setup packet bit is set to one, but no connection setup segment is found — X'A01BFF0D'.

FF0D
RTP received a packet in which the RTP transport header did not contain a required optional segment or control vector. *nn* is the key of the missing optional segment or control vector. One of the following error conditions was detected:

- The TCID assignor bit is set to one, the connection qualifier/source identifier field present bits are set to 01, but no network address (X'05') control vector is present — X'A01BFF05'.
- No active context is found, the setup packet bit is set to one, but no connection setup segment is found — X'A01BFF0D'.

FF14
RTP received a packet in which the RTP transport header did not contain a required optional segment or control vector. *nn* is the key of the missing optional segment or control vector. One of the following error conditions was detected:

- The TCID assignor bit is set to one, the connection qualifier/source identifier field present bits are set to 01, but no network address (X'05') control vector is present — X'A01BFF05'.
- No active context is found, the setup packet bit is set to one, but no connection setup segment is found — X'A01BFF0D'.

FFXX (HPR sense data)

Category and modifier (in hexadecimal):

FF00
HPR routing failed or not required.

Bytes 2 and 3 following the sense code contain sense-code-specific information.

0001
HPR routing not required.

0002
HPR routing failed.

FF10
Values not defined.

0001
Route values not defined.

FF20
Problem with connection setup signal.

0001
Connection setup signal not present.

FF30
Route setup record not found or has an error.

0001
Route setup record not found.

0002
Route setup record found, but has an error.

FF50
ADJCP not found.

0001
ADJCP not found.

0002
Survivable CV46 error set when CPNAME in CV46 is the same as CPNAME in CV44.

0003
VRBLK not found.

FF60
DLC NCB not found.

0001
DLC NCB not found.

0002
DLC NCB was found, but the reuse count was wrong.

FF70
RTP ALS not found or address failed.

0001
RTP ALS not found.

0002
RTP ALS network address in use.

0003
RTP ALS CIDCTL ADD HOSTNODE failed.

0004
RTP ALS state change in progress.

0005
RTP ALS CIDCTL ADD NEXTNODE failed.

0006
RDTADD new address failed.

0007
Our NCE Instance Identifier has changed.

0008
SLOCATE failed.

0009
During Route_Setup processing, an intermediate node on the Route_Setup path forced the RTP being established to terminate on that node due to locally defined restrictions that do not allow RTPs to pass through that node. This condition should not lead to a Route_Setup failure, but instead should result in back-to-back RTPs being established at this node (rather than a single RTP that passes through this node).

FF80
RTP NCB not found or not valid.

0001
RTP NCB not found.

0002
RTP NCB state not valid.

0003
Route_Setup RTP pending.

0004
Route_Setup RTP not useable.

0005
Route_Setup RTP not found.

FF90
MNPS RECOVERY stop.

0001
MNPS RECOVERY stop.

FFC8
HPR/IP (Enterprise Extender) getaddrinfo error.

0001
Hostname not found.

0002
Try again–temporary error.

0003
Unrecoverable error occurred.

0004
HPR/IP (Enterprise Extender) addressing keys (LSAP, RSAP, IPADDR) duplicate those of a preexistent connection.

VTAM hint: Check the SAPADDR statements. They must be unique for each connection. See z/OS Communications Server: SNA Network Implementation Guide for more information about HPR/IP (Enterprise Extender) addressing.

0005
Hostname length error.

0006
getaddrinfo timeout.

SNA sense field values for RPL-based macroinstructions

When the application program or a logical unit receives an exception request, a negative response, or a logical unit status (LUSTAT) request, the associated sense data includes information regarding the reason for the exception condition. There are three types of information that describe the exception condition:

- System-sense information
- System-sense modifier information
- User-sense information

System sense information indicates one of the five major classes of system-defined errors.

System-sense modifier information indicates one of many specific causes of the error indicated by the system-sense information. Like RTNCD and FDB2, the system-sense and its modifier information together form a specific type of error condition within a general class of error conditions.

User-sense information is generally used when the error condition is detected by the user-written program itself. In general, no particular codes or values are defined by IBM to indicate types of errors. The logical unit must generate its own user-sense information that is understood by other logical units.

The SNA defined values for the sense fields can be found in the *SNA Formats*. Additional information is contained in the *SNA Format and Protocol Reference Manual: Architectural Logic,* and the *SNA Sessions between Logical Units*.

These three types of sense information—system, system modifier, and user—are set in RPL fields. Three fields (one for each type of sense information) are set by the application program when it sends a negative response or LUSTAT request to the logical unit. Three other fields are set by VTAM when the application program receives an exception request, a negative response, or LUSTAT request from the logical unit. These are the names of the six fields, as they would be used on a manipulative or RPL macro:

Sense information	**Received by the application program**	**Sent from the application program**
System-sense information	SSENSEI	SSENSEO
System-sense modifier information	SSENSMI	SSENSMO
User-sense information	USENSEI	USENSEO

System-sense information

The values that are set in the system-sense field are predefined by IBM. These values are as follows (the operands shown here are those used with a MODCB or TESTCB macro; the corresponding hexadecimal value is also shown in parentheses):

Table 2. Sense field values

System-sense values	**Meaning**
SSENSEI=PATH (X'80')	A path error occurred. The RU could not be delivered to the intended receiver because of a physical problem in the network path or an error in the system-supplied transmission header that accompanied the RU. If no recovery action is possible, terminate the session with the logical unit.
SSENSEI=CPM (X'40')	An unrecoverable request header error occurred.
SSENSEO=CPM (X'40')	The sender did not correctly enforce the current session protocols. Terminate the session with the logical unit.
SSENSEI=STATE (X'20') SSENSEO=STATE (X'20')	A state error occurred in the application program's or logical unit's use of sequence numbers, chaining indicators, bracket indicators, or change-direction indicators. A state error can also occur when a data-flow-control request is issued, data is sent after a clear request, or when a session-control request is issued before a clear request. This type of error is recoverable; use clear, STSN, and SDT requests.
SSENSEI=FI (X'10') SSENSEO=FI (X'10')	A request error occurred. The application program or logical unit cannot handle the request because the request itself is not valid. This error might be recoverable.
SSENSEI=RR (X'08') SSENSEO=RR (X'08')	A request reject occurred. The request was delivered to the intended receiver; it was correctly interpreted, but not handled by the receiver. This might be a recoverable condition.

3270 SNA and non-SNA device sense fields

Table 3 on page 145 and Table 4 on page 145 provide information on sense fields for a 3270 SNA or non-SNA device. See z/OS Communications Server: SNA Programming for information about programming for the IBM 3270 Information Display System.

Table 3. SNA sense information received at the application program

SNA sense	SNA definition	Cause for exception
80*xxyyyy*	Path error	Request could not be delivered [1]
400A0000	No-response not allowed	RESPOND=(NEX,NFME,NRRN)
400B0000	Chaining not supported	CHAIN=(FIRST or MIDDLE or LAST)
20030000	Bracket state error	BRACKET=NBB and no bracket currently exists [2]
20010000	Sequence number error	Session sequence number error
10030000	Function not supported	CONTROL=(DATA or CLEAR)
10000020	Request error	Command rejected
08210000	Session parameter not valid	Parameters not valid in BIND
08130000	Bracket bid reject—No RTR Forthcoming	BRACKET=BB and a bracket already exists [2]
0000*zzzz*	Other exception	Device exception—USENSEI values are defined in Table 4 on page 145

Note:

1. *xx* is defined in *SNA Formats*. For a PU type 1 3270 terminal, *yyyy* can be set to 0010 (intervention required). For a BSC 3270 terminal attached to a communication controller, *yyyy* represents the NCP system response byte and extended response byte returned for some path error conditions. For information on how these bytes are defined, see *NCP and EP Ref. Summary and Data Areas, Volumes I and II*.
2. This sense code applies only if bracket protocols are being used in the session.

Table 4. Explanation of USENSEI Information

USENSEI Byte 0								USENSEI Byte 1								Meaning
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	
.	.	.	.	X	.	.	.	.	.	.	.	.	.	.	.	Device busy
.	.	.	.	.	X	.	.	.	.	.	.	.	.	.	.	Unit specify
.	.	.	.	.	.	X	.	.	.	.	.	.	.	.	.	Device end
.	.	.	.	.	.	.	X	.	.	.	.	.	.	.	.	Transmission check
.	.	.	.	.	.	.	.	.	.	X	.	.	.	.	.	Command rejected
.	.	.	.	.	.	.	.	.	.	.	X	.	.	.	.	Intervention required
.	.	.	.	.	.	.	.	.	.	.	.	X	.	.	.	Equipment check
.	.	.	.	.	.	.	.	.	.	.	.	.	X	.	.	Data check or bus-out check
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	X	Operation check
X	X	X	X	.	.	.	.	X	X	.	.	.	.	.	.	Reserved

Table 4. Explanation of USENSEI Information (continued)		
USENSEI Byte 0	**USENSEI Byte 1**	**Meaning**
Note: Transmission check is indicated for a channel-related error (such as PCI, channel program check, protection check, channel data check, channel control check, interface control check, or chaining check) for a channel-attached non-SNA 3270.		

The application program can disobey the LU Type 0 protocols by attempting to send:

- A data-flow-control request
- A response
- A request indicating other than a single-request chain
- A request that does not ask for a definite or exception response Type 1 (FME)

If you attempt any of the preceding items, the following results occur, depending upon the actual type of terminal used in the session:

- The SEND macro is rejected with (RTNCD,FDB2)=(X'14',X'47').
- VTAM returns a negative response.
- VTAM ignores the protocol violation, and unpredictable results can occur.

Chapter 2. Return codes for VTAM macroinstructions

This chapter provides information about return codes for macros that are displayed in VTAM messages and contains the following sections:

- "ACB OPEN and CLOSE macroinstruction error fields" on page 147
- "RPL RTNCD and FDB2 return code combinations" on page 151
- "RTNCD and FDB2 information for LU 6.2" on page 170
- "RCPRI and RCSEC return codes for LU 6.2" on page 172.
- "LAN channel station error return codes" on page 206

ACB OPEN and CLOSE macroinstruction error fields

This section contains only error fields for the ACB OPEN and CLOSE macros. See z/OS Communications Server: SNA Programming for a description of the OPEN and CLOSE macros or for information on other macros.

OPEN macroinstruction error fields

A list of the values that can be set in the ERROR field of an ACB follow (ACBERFLG is the actual field name). See z/OS Communications Server: SNA Programming for a description of the OPEN macro.

0 (X'00')
OPEN successfully opened this ACB.

4 (X'04')
The ACB has been opened.

20 (X'14')
OPEN cannot be processed because of a temporary shortage of storage.

36 (X'24')
The OPEN ACB failed for one of the following reasons:

- The password specified by the ACB did not match the corresponding password in the APPL entry.
- The ACB did not specify a password and the APPL contains one.
- The security management product determined that the user is not authorized to open the ACB.

70 (X'46')
OPEN was issued in an exit routine.

80 (X'50')
VTAM has not been included as part of the operating system. The fault lies in the system definition procedures.

82 (X'52')
VTAM is included as part of the operating system, but the VTAM operator issued a HALT command, and VTAM has shut down. You cannot attempt to establish a session or communicate with any LUs.

84 (X'54')
Either the address supplied in the ACB's APPLID field lies beyond the addressable range of your application program, or no entry is found in the VTAM configuration tables that matches the name indicated by the ACB's APPLID field (or supplied by the operating system). If the OPEN macro is specified correctly, your system programmer might have:

- Failed to include your application program's symbolic name during VTAM definition
- Improperly handled the symbolic name

See the description of the APPLID operand in the ACB macro.

© Copyright IBM Corp. 2000, 2021

86 (X'56')
A match for your application program's symbolic name is found, but it is for an entry other than an APPL. If you specified this name in the ACB's APPLID field, verify that you have the correct name and handled this name properly (see the APPLID operand of the ACB macro). If the symbolic name is supplied by the operating system, the supplied name is suspect.

88 (X'58')
Another ACB, already opened by VTAM, indicates the same application program symbolic name that this ACB does. The system programmer might have assigned the same symbolic name to two application programs. This is valid only if the programs are not open concurrently. Possibly the system operator initiated your program at the wrong time.

For multinode persistent session support, an MNPS takeover OPEN was rejected by the owning VTAM node.

90 (X'5A')
No entry is found in the VTAM configuration tables that matches the name indicated by the ACB APPLID field (or supplied by the operating system). This error might have occurred for one of the following reasons:

- The VTAM operator deactivated the APPL entry
- The APPL entry was never created
- VTAM is trying to recover for persistent sessions and the application is not in pending recovery state

92 (X'5C')
VTAM is included as part of the operating system but inactive.

94 (X'5E')
The address supplied in the ACB APPLID field lies beyond the addressable range of your application program.

95 (X'5F')
The VTAM transient being used by the application for an OPEN ACB does not match the level of VTAM. The correct level of VTAM is not in the LIBDEF search chain for the application.

96 (X'60')
An apparent system error occurred. Either there is a defect in VTAM logic, or there is an error in your use of OPEN or CLOSE that VTAM did not properly detect. Save all applicable program listings and storage dumps, and consult your IBM programming services representative.

98 (X'62')
The APPLID length byte is incorrectly specified.

100 (X'64')
The address supplied in the ACB's PASSWD field lies beyond the addressable range of your application program.

102 (X'66')
The PASSWD length byte is incorrectly specified.

104 (X'68')
The APPLID field in the ACB identifies an application program that is defined with AUTH=PPO in its APPL definition statement. Another program with the same authorization is active. Only one program defined with AUTH=PPO can be active at a time.

106 (X'6A')
The address supplied in the ACB's vector list field lies beyond the addressable range of your application program.

108 (X'6C')
The ACB vector list length byte is incorrectly specified.

112 (X'70')
You attempted to open an ACB that is in the process of being closed. This can occur when a VTAM application program job step or subtask is canceled or terminates abnormally. The process of closing the ACB can continue after the job step or subtask has actually terminated. Subsequently, if the job

step is restarted or the subtask is reattached before the ACB closing process has been completed, an OPEN macro that is then issued for that ACB fails.

114 (X'72')
This code occurs from an open ACB failure for the VTAM CP when VERIFYCP is coded as a start option or for an OPEN ACB failure for an LU 6.2 application with VERIFY=OPTIONAL or VERIFY=REQUIRED for one of the following reasons:

- The security management product is not installed.
- The security management product is not active.
- The security management product resource class APPCLU is not active.
- The application represented by the ACB is not in the security management product Started Procedures Table.

116 (X'74')
VTAM rejected the takeover by an alternate application because the original application did not enable persistence, although it is capable of persistence.

118 (X'76')
OPEN failed for one of the following reasons:

- The specified application is in a recovery pending state and PERSIST=YES is not specified on the ACB that is being opened
- The application is in pending terminate state and an active CDRSC with the same name has been found in the sysplex

120 (X'78')
ACB or APPL statement option mismatch between original application and opening takeover or recovery application. One or more of the following situations can apply:

- APPC mismatch—both application APPL statements must specify either APPC=YES or APPC=NO; they cannot differ.
- ENCR or MAC mismatch—the recovering application APPL statement must specify a security level equal to or higher than the setting in effect for the original application.
- ENCRTYPE mismatch—the recovering application APPL statement must specify a minimum encryption level equal to or higher than the setting in effect for the original application.
- FDX mismatch—both applications must be specified as FDX=YES or FDX=NO; they cannot differ
- GNAME capability mismatch—the original application was supporting a generic name but the VTAM node of the recovering application is not connected to a generic resource structure or its structure name differs from the original structure name.
- ISTVAC81 vector mismatch—the application capabilities vector provided by the recovering application does not match that of the original application.
- LIMQSINT mismatch—both application APPL statements must agree in their specification of a LIMQSINT parameter; either both must specify a value or neither must specify a value. However, the actual timer values specified do not need to be identical.
- MACRF mismatch—both values must be either LOGON or NLOGON; they cannot differ.
- NQNAMES mismatch—both applications must be specified as NQNAMES=YES or NQNAMES=NO; they cannot differ.
- PERSIST mismatch—both applications must be specified as PERSIST=YES or PERSIST=NO; they cannot differ.
- SECLVL mismatch—both application APPL statements must specify the same SECLVL setting values; they cannot differ.
- VERIFY mismatch—both application APPL statements must specify the same VERIFY setting values; they cannot differ.

122 (X'7A')
The OPEN ACB issued by a monitor application was rejected because a monitor application was already active on this VTAM.

124 (X'7C')
The OPEN ACB that would have resulted in SNPS takeover processing was rejected because the active application does not support SNPS takeover requests.

188 (X'BC')
The ACB is in the process of being opened or closed by another request.

244 (X'F4')
The application program is not authorized for SRBEXIT=YES. A request to open an ACB whose corresponding APPL definition statement specifies SRBEXIT=YES is rejected unless the application program is APF authorized, or using key 0–7, or in supervisor state.

246 (X'F6')
NIB storage address not valid. A CNM authorized application program either failed to supply an NIB pointer in the NIB field of the ACB, or the NIB address supplied lies beyond the addressable range of the application program.

250 (X'FA')
NIB options not valid. Either an application program without CNM authorization (specified in its associated VTAM resource definition) supplied an NIB pointer in its ACB; or, if CNM authorized, the application program failed to supply valid NIB options on the NIB macro.

254 (X'FE')
Duplicate unsolicited RU routing requested. The CNM routing table indicated that this application program was to receive the same unsolicited formatted requests that were already being routed to another active CNM authorized application program. Only one application program can be actively receiving a particular type of RU (for example, RECFMS) at a time.

CLOSE macroinstruction error fields

A list of the values that can be set in the ERROR field of an ACB follow (ACBERFLG is the actual field name). See z/OS Communications Server: SNA Programming for a description of the CLOSE macro.

0 (X'00')
CLOSE successfully closed the ACB.

4 (X'04')
A CLOSE macro has been successfully issued for this ACB (or the ACB has never been opened in the first place).

20 (X'14')
CLOSE cannot be processed because of a temporary shortage of storage.

64 (X'40')
Outstanding OPNDST OPTCD=ACQUIRE is not released.

66 (X'42')
The ACB has been closed, but an apparent system error has prevented the successful termination of one or more of the sessions that the application program has. It is VTAM fault; consult your IBM Program Support Representative. The LUs that have not had their sessions terminated are not available to other application programs, and LUs with which you were requesting a session when CLOSE was executed are likewise unavailable. You can notify the VTAM operator (during program execution) of the situation so that the operator can make the LUs available to other application programs.

70 (X'46')
CLOSE was not issued in the mainline program. OPEN and CLOSE cannot be issued in any exit routine.

76 (X'4C')
This application program is authorized to issue VTAM operator commands and receive VTAM messages. A CLOSE was issued, but messages are still queued for it, or VTAM is waiting for a reply,

or both. See z/OS Communications Server: SNA Programming for information about closing program operators.

80 (X'50')
VTAM is no longer included as part of the operating system.

96 (X'60')
An apparent system error occurred. Either there is a defect in VTAM logic, or there is an error in your use of OPEN or CLOSE that VTAM did not properly detect. Save all applicable program listings and storage dumps, and consult your IBM programming services representative.

112 (X'70')
CLOSE was issued while the program was in the process of terminating abnormally. The CLOSE is not necessary because the ACB is closed by VTAM when the task terminates.

188 (X'BC')
The ACB is in the process of being opened or is in the process of being closed by another request.

RPL RTNCD and FDB2 return code combinations

This section describes all the RTNCD-FDB2 combinations that can be set in an RPL when it is posted complete. See z/OS Communications Server: SNA Programming for information about return code posting.

RTNCD	FDB2	Explanation
0	0	Normal completion or request accepted

The operation has been completed normally or the request has been accepted.

RTNCD	FDB2	Explanation
0	5	Input area too small

You issued INQUIRE, INTRPRET, or OPNDST OPTCD=RESTORE and specified an input work area that is too small. VTAM has placed the required length (in bytes) in the RPL's RECLEN field (for INQUIRE) or ARECLEN (for INTRPRET). No data has been placed in the work area.

Obtain a work area that is at least as long as the value set in RECLEN or ARECLEN, place the length in the AREALEN field (for INQUIRE) or AAREALN (for INTRPRET), and reissue INQUIRE or INTRPRET.

RTNCD	FDB2	Explanation
0	6	No input available

A RECEIVE OPTCD=NQ was issued and there was no input of the specified RTYPE available to satisfy the macroinstruction, or a RCVCMD OPTCD=NQ was issued and there was no input available to satisfy the macroinstruction.

RTNCD	FDB2	Explanation
0	7	INQUIRE information not available

One of the following situations has occurred:

- You issued INQUIRE OPTCD=LOGONMSG to obtain user data (a logon message) from a queued CINIT and there is no queued CINIT.
- You issued INQUIRE OPTCD=SESSPARM to obtain session parameters from a queued CINIT and there is no queued CINIT.
- You issued INQUIRE OPTCD=SESSKEY to obtain the session cryptography key, and there is no session cryptography key.
- You issued INQUIRE OPTCD=DEVCHAR for a cross-domain resource.

- You issued INQUIRE OPTCD=TOPLOGON for queued CINITs, and there are no queued CINITs.
- You issued INQUIRE OPTCD=CIDXLATE for a session that has not been established.
- You issued an INQUIRE OPTCD=USERVAR and no USERVAR was defined.
- You issued an INQUIRE OPTCD=PERSESS, and no record application program interface sessions are pending recovery.

The problem might be due to an incorrectly set NAME field in the NIB, an CID that is not valid in the NIB or RPL, a failure on the part of the system programmer to create the appropriate entry during VTAM definition, or a VARY command issued by the VTAM operator that deactivated the entry.

RTNCD	FDB2	Explanation
0	8	OPNDST OPTCD=ACQUIRE, SIMLOGON, or CLSDST OPTCD=PASS failed

An OPNDST OPTCD=ACQUIRE or SIMLOGON OPTCD=NQ failed for one of the following reasons: the requested logical unit is at its session limit or is not enabled for sessions in which it is to be the SLU. See z/OS Communications Server: SNA Programming for a description of OPNDST and SIMLOGON.

A SIMLOGON OPTCD=Q failed because the requested logical unit is at its session limit and at least one of its current sessions is with the application program that issued the SIMLOGON.

A CLSDST OPTCD=PASS failed for one of two reasons. There is already a queued session between the logical unit being passed and the target primary logical unit, or you attempted to initiate or pass the session to the same PLU APPL.

RTNCD	FDB2	Explanation
0	9	OPNDST OPTCD=ACCEPT denied (no queued CINITs) or OPNDST OPTCD=RESTORE denied (no sessions restored)

You attempted to accept a session and indicated that your request should be rejected if no pending active session is waiting to be accepted (OPTCD=NQ). The request is rejected because no CINIT is queued for your application program.

An OPNDST OPTCD=RESTORE failed because the sessions that are requested are not pending recovery. None of the sessions specified by the NIBLIST are restored.

RTNCD	FDB2	Explanation
0	10(X'0A')	Application program not connectable

You issued INQUIRE OPTCD=APPSTAT to check an application program's ability to establish sessions. The application program is in an inactive, non-connectable state because the VTAM operator deactivated it. Therefore, the application program is not available for sessions.

RTNCD	FDB2	Explanation
0	11(X'0B')	Conditional Completion for APPCCMD

Some type of error might have occurred on an APPCCMD macroinstruction. For further problem determination, refer to the primary and secondary return codes in the RPL extension. See the z/OS Communications Server: SNA Programmer's LU 6.2 Reference for further information.

RTNCD	FDB2	Explanation
0	13(X'0D')	Additional sessions pending recovery

You have issued INQUIRE PERSESS and specified an input work area that is too small. VTAM fills the work area with as much information as possible and places the length used in the RPL's RECLEN. The INQUIRE must be reissued to recover the remainder of the information.

RTNCD	FDB2	Explanation
4	3	Exception request received

An exception request has been received. The reason for the exception is contained in the RPL's SSENSEI, SSENSMI, and USENSEI fields. If a negative response has not been sent to a request of this chain and if this request (the exception request) requires a response, move the input sense fields to the output sense fields and send a negative response. All requests in the current chain that have been received by the application program should be discarded. If the current request did not end the chain, issue RECEIVE macroinstructions with OPTCD=TRUNC and AREALEN=0 until CHAIN=LAST or CONTROL=CANCEL is received. No responses should be sent for any request in the rest of the chain.

RTNCD	FDB2	Explanation
4	4	Negative response received

The logical unit (or some other node in the network) has sent a response indicating that an exception condition was detected for one of the requests that the application program sent on this session. The SEQNO field indicates the sequence number of the request to which the negative response applies. The SSENSEI, SSENSMI, and USENSEI fields indicate the reason for the exception condition.

See z/OS Communications Server: SNA Programming for more information on the SEQNO field, and the SSENSEI, SSENSMI, and USENSEI fields.

If the request with which the negative response is associated is part of an incomplete chain currently being transmitted to the logical unit, the application program should terminate the chain by issuing a SEND STYPE=REQ, CONTROL=DATA, CHAIN=LAST or a SEND STYPE=REQ, CONTROL=CANCEL to indicate that the logical unit can stop discarding the requests it is receiving. Refer to z/OS Communications Server: SNA Programming for information about the use of STSN and CLEAR to alter sequence numbers. Also see the discussion of (RTNCD,FDB2)=(12,13) in this section.

RTNCD	FDB2	Explanation
4	5	Symbolic name known in this SSCP by its network-qualified name only

A real-to-symbolic translation request is made, and NIBNET is filled in with a network identifier, but VTAM cannot provide a symbolic name. VTAM knows this resource only by its network-qualified name; there is no symbolic name that represents this resource. Do one of the following actions:

- Use the network-qualified name
- Define a symbolic name to represent this resource.

RTNCD	FDB2	Explanation
8	0	Temporary storage shortage

VTAM is temporarily unable to secure enough storage to process the request. The request can usually be reissued (with EXECRPL, for example). For applications running at a priority near to or higher than VTAM's priority, the application should wait a brief time before trying this again.

In certain cases, the macroinstruction processing has not gotten far enough to have done significant work, and the request can be reissued. In other cases, the processing might have gone beyond some irreversible point before failing; as a result, the request cannot simply be reissued. For example, if the LOGON exit routine has been scheduled with a CINIT request and OPNDST OPTCD=ACCEPT is issued, the OPNDST operation can fail before responding to the CINIT, in which case the OPNDST can simply be reissued. If the response to CINIT had been sent, however, and then storage could not be obtained, the OPNDST request could not be reissued as there would no longer be a CINIT to accept. In this case, the application program might wish to initiate another session between itself and the LU, perhaps by using

SIMLOGON. These two cases can be distinguished by a bit in the NIB; when the OPNDST OPTCD=ACCEPT is posted, NIBNACLQ is 1 if the response to CINIT is sent; otherwise it is 0.

RTNCD	FDB2	Explanation
12(X'0C')	10(X'0A')	Request canceled by RESETSR

This RECEIVE operation has been canceled by a RESETSR macroinstruction issued by another part of your application program.

RTNCD	FDB2	Explanation
12(X'0C')	11(X'0B')	Request canceled because the session has been terminated

The request has been canceled because the session was terminated. Session termination always cancels any pending requests for the session, and returns this return code in the RPL. See z/OS Communications Server: SNA Programming for a list of the possible causes of session termination.

This return code is also used when an OPNDST OPTCD=(ACCEPT,SPEC,Q) is canceled by CLSDST.

RTNCD	FDB2	Explanation
12(X'0C')	12(X'0C')	Request canceled by CLEAR request

While the RPL-based request was being processed, a CLEAR request was sent or received on the session. This stops all data flow and cancels all pending communication requests on the session. The CLEAR request might have been sent by your application program (SESSIONC macroinstruction), or the request might have been sent on behalf of your application program by VTAM. The CLEAR request might also have been sent from the other end of the session.

RTNCD	FDB2	Explanation
12(X'0C')	13(X'0D')	Prior exception in chain detected

A series of chained requests was being sent to the logical unit and a negative response was returned for one of them. All subsequent SEND macroinstructions for that chain are posted complete with this return code; however, for each such SEND, the associated request unit is sent on the session to the session partner where it should be discarded.

RTNCD	FDB2	Explanation
12(X'0C')	14(X'0E')	Request cancelled - POA queue limit exceeded

The POA issued a SENDCMD after it reached its queue limit (POAQLIM on the APPL definition statement). Subsequent SENDCMDs complete with this return code until you receive all of the messages in the queue. You can empty the message queue by issuing RCVCMD OPTCD=NQ (no queue) until an RCVCMD completes with a return code and feedback of X'0006'. A SENDCMD now returns successfully.

RTNCD	FDB2	Explanation
16(X'10')	0	Logical unit not available, application program status not available, queued BIND not available, or incorrect dial parameters

This code is set for one of the following reasons:

- You are attempting to establish a session with a logical unit that is not active.
- You are attempting to pass a logical unit to a primary logical unit that is not active (or is in the process of being deactivated).
- You are attempting to issue an OPNSEC macroinstruction and there is no queued BIND request to respond to.

- You are attempting to determine the status of an application program that is in another domain, the status is not available, and your application program has to proceed without it.
- You issued a SIMLOGON macroinstruction that specifies dial parameters for a nonswitched PU.
- The dial parameters specified in the SIMLOGON macroinstruction do not match the original dial parameters.
- You issued a macroinstuction and a resource, such as a network address or storage, was not available. A sense code is returned in the RPL containing specific information.

The RPL system-sense (SSENSEI), the system-sense modifier (SSENSMI), and the user-sense (USENSEI) can contain a more detailed explanation of the failure.

RTNCD	FDB2	Explanation
16(X'10')	1	OPNDST failed

OPNDST failed; if a session had been established by the OPNDST, it has now been terminated. Some reasons for OPNDST failure are as follows:

- No network path could be obtained. For example, there might have been a failure of the virtual route or route extension, or the operator might have deactivated a network component along the path.
- A dial connection was not completed.
- A negative response to a CRV request was received.
- A request rejected response to a BIND request was received.
- The logical unit does not exist.
- A BIND response that is not valid was received; for example, a negotiable BIND response was received for a non-negotiable BIND request.
- OPNDST OPTCD=ACQUIRE specifies dial parameters for a nonswitched PU.
- The dial parameters specified in the OPNDST OPTCD=ACQUIRE do not match the original dial parameters.

The SSENSEI, SSENSMI, and USENSEI fields are set; these fields are described in “SNA sense field values for RPL-based macroinstructions” on page 143.

RTNCD	FDB2	Explanation
16(X'10')	2	Logical unit inhibited for sessions

You attempted to initiate a session and one of the logical units in the requested session is inhibited. For example, a VTAM application program is inhibited for sessions if it issues SETLOGON OPTCD=QUIESCE or has never issued SETLOGON OPTCD=START. Refer to z/OS Communications Server: SNA Programming for more information.

RTNCD	FDB2	Explanation
16(X'10')	3	HALT issued

The VTAM operator has issued a HALT command. Depending on the type of HALT, certain macroinstructions can no longer be issued by your application program. Refer to z/OS Communications Server: SNA Programming for more information.

RTNCD	FDB2	Explanation
16(X'10')	5	Request or response encryption failure

Encryption has failed while:

- Sending an FM data request
- Sending the BIND response during OPNSEC processing

- Sending the CRV request during OPNDST processing.

RTNCD	FDB2	Explanation
16(X'10')	7	Request canceled by VARY command

The communication operation has been canceled because the VTAM operator deactivated a necessary portion of the path while the macroinstruction was being processed. If a LOSTERM exit routine is available, it has been scheduled. You can no longer communicate with the LU, and you should issue CLSDST to terminate its session with your application program.

RTNCD	FDB2	Explanation
16(X'10')	9	Unconditional Terminate or character-coded logoff received

The logical unit has sent an unconditional Terminate request or a character-coded logoff that is a request for unconditional session-termination. No further communication on the session is possible. CLSDST must be issued.

RTNCD	FDB2	Explanation
16(X'10')	10(X'0A')	VTAM error

An error occurred in VTAM itself. No further attempts to establish or terminate a session with the logical unit should be made.

RTNCD	FDB2	Explanation
16(X'10')	13(X'0D')	VTAM inactive for your ACB

The association between VTAM and your application program (ACB) that was established with OPEN has been broken; the ACB is in the process of being closed. This might have occurred because you have elsewhere issued a CLOSE that has not yet completed, or it might have occurred because VTAM has become inactive, or a VARY INACT was issued for your application program.

RTNCD	FDB2	Explanation
16(X'10')	14(X'0E')	Request abnormally terminated

VTAM has abnormally terminated a request because of an error detected while processing the request or because of an error in the associated session, task, or address space (for example, an abend). See z/OS Communications Server: SNA Programming for more information about error isolation and recovery.

RTNCD	FDB2	Explanation
16(X'10')	15(X'0F')	Buffers filled

Previously VTAM had received an RU; the application program did not have an appropriate EXLST exit routine or outstanding RECEIVE for the RU and there was no buffer space left for VTAM to queue the RU. Under these circumstances, VTAM discards that RU and any other RUs queued for the session and schedules the LOSTERM exit routine (if there is one) with reason code 36. If appropriate for the TS Profile for this session, a Clear is sent to the session partner. In all cases, the end of the session that experienced the buffer shortage is put into data-traffic-reset state (at least momentarily). Any SEND or RECEIVE issued while the session is in this state is rejected with (RTNCD,FDB2)=(X'10',X'0F'). This mode of operation continues until a Start Data Traffic response is processed (or until the Clear function completes, if SDT is not appropriate for the TS profile).

RTNCD	FDB2	Explanation
16(X'10')	17(X'11')	SDT failure on OPNDST

A negative response was sent by a logical unit in reply to a Start Data Traffic (SDT) request. The OPNDST was not completed successfully. The SSENSEI, SSENSMI, and USENSEI fields are set; these fields are described in “SNA sense field values for RPL-based macroinstructions” on page 143.

RTNCD	FDB2	Explanation
16(X'10')	18(X'12')	Macroinstruction failure, sense included

A REQSESS, TERMSESS, or OPNSEC has failed. A sense code (SSENSEI, SSENSMI, and USENSEI field) is returned in the RPL for the failing macroinstruction.

RTNCD	FDB2	Explanation
16(X'10')	19(X'13')	Attempt to start LU 6.2 session request rejected

An LU 6.2 application has tried to start an LU 6.2 session independent of VTAM. No pending sessions have been disturbed. This occurs when an OPNDST is issued with an LU 6.2 user-specified BIND.

RTNCD	FDB2	Explanation
16(X'10')	20(X'14')	Attempt to start LU 6.2 session pending session terminated

An LU 6.2 application has tried to start an LU 6.2 session independent of VTAM. The pending session has been terminated. This occurs when the LOGMODE specified on an OPNDST resolves to an LU 6.2 BIND or when OPNSEC is issued for an LU 6.2 BIND.

RTNCD	FDB2	Explanation
16(X'10')	21(X'15')	An APPCCMD must be issued

An OPNDST or CLSDST has been issued for a pending LU 6.2 session. An APPCCMD CONTROL=OPRCNTL, QUALIFY=ACTSESS or QUALIFY=DACTSESS macroinstruction must be issued for this session. See the z/OS Communications Server: SNA Programmer's LU 6.2 Reference for more information.

RTNCD	FDB2	Explanation
16(X'10')	22(X'16')	Specified LU is nonswitched

The application issues a SIMLOGON or OPNDST OPTCD=ACQUIRE macroinstruction using the application supplied dial-out function. The specified LU is nonswitched and the request failed.

RTNCD	FDB2	Explanation
16(X'10')	23(X'17')	Encryption not allowed

You attempted to request encryption on a send, but session does not support encryption.

RTNCD	FDB2	Explanation
16(X'10')	24(X'18')	Sysplex is inaccessible

You attempted to use either the INQUIRE OPTCD=SESSNAME, SETLOGON OPTCD=GNAMEADD, SETLOGON OPTCD=GNAMEDEL, SETLOGON OPTCD=GNAMESUB, OPNDST, OPNSEC, or the CHANGE OPTCD=ENDAFFIN macroinstruction, but the coupling facility for this host is inaccessible.

RTNCD	FDB2	Explanation
16(X'10')	25(X'19')	Host is not member of Sysplex

The application issued either the INQUIRE OPTCD=SESSNAME, the CHANGE OPTCD=ENDAFFIN, or the SETLOGON OPTCD=GNAMEADD|GNAMEDEL|GNAMESUB macroinstruction, but the coupling facility for this host is inaccessible. The coupling facility might be inaccessible because:

- A coupling facility does not exist.
- A CFRM policy for the required coupling facility structure was not active.
- VTAM is not defined as an APPN node.
- VTAM has lost connectivity to the required coupling facility structure.

RTNCD	FDB2	Explanation
16(X'10')	26(X'1A')	SUSPEND failed

VTAM attempted to SUSPEND an RPL request issued in either cross-memory mode or in synchronous SRB mode with OPTCD=KEEPSRB specified. The attempt failed.

RTNCD	FDB2	Explanation
16(X'10')	27(X'1B')	RESUME failed

VTAM attempted to RESUME an RPL request issued in either cross-memory mode or in synchronous SRB mode with OPTCD=KEEPSRB specified. The attempt failed. VTAM is unable to post the request complete. If the application has a LOSTERM exit, it will be scheduled with a reason code of 44.

For more information about the LOSTERM exit, see the z/OS Communications Server: SNA Programming. The RPL is now available for reuse.

RTNCD	FDB2	Explanation
16(X'10')	28(X'1C')	OS level does not support requested function

A macroinstruction request required the use of an operating system service which is not supported by the active operating system level.

RTNCD	FDB2	Explanation
16(X'10')	29(X'1D')	Security Manager Error

An error was encountered when attempting to invoke the security management program. The APPL definition statement for this application specifies VERIFY=REQD or VERIFY=OPTIONAL, indicating that the use of an installed security manager was required for APPC sessions by this application program. However, VTAM was unable to successfully invoke the security manager. The SETLOGON START macroinstruction is rejected.

RTNCD	FDB2	Explanation
20(X'14')	0	VSAM request

The RPL contains a VSAM or other non-VTAM request code. No ECB has been posted and no RPL exit routine has been scheduled.

RTNCD	FDB2	Explanation
20(X'14')	2	Zero EXIT field

The RPL indicates that the ECB-EXIT field is being used as an EXIT field, but the RPL exit routine address in it is 0. No RPL exit routine has been scheduled.

RTNCD	FDB2	Explanation
20(X'14')	3	Zero ECB field

The RPL indicates that the ECB-EXIT field is being used to point to an external ECB, but the address in the field is 0. No ECB has been posted.

RTNCD	FDB2	Explanation
20(X'14')	4	Inactive RPL checked

CHECK was issued for an inactive RPL (an RPL that had been posted complete and for which CHECK has already been issued successfully). All RPL-based macroinstructions must use an inactive RPL. All CHECK macroinstructions, however, must use an active RPL; an RPL cannot be checked twice.

RTNCD	FDB2	Explanation
20(X'14')	16(X'10')	Control block not valid

The RPL's ACB field does not contain the address of a valid ACB or the ACB is closed. This can mean that the ACB field of the RPL was incorrectly set or the ACB has been destroyed.

RTNCD	FDB2	Explanation
20(X'14')	17(X'11')	RTYPE not valid

A RECEIVE has been issued with the RTYPE field set to NDFSYN, NDFASY, and RESP.

RTNCD	FDB2	Explanation
20(X'14')	18(X'12')	CLSDST in progress

At the time this macroinstruction was executed, a CLSDST request was pending for the session. The CLSDST request takes priority, and the request that received this return code cannot be honored.

RTNCD	FDB2	Explanation
20(X'14')	19(X'13')	CID not valid

The RPLARG field or the NIBCID field does not contain a valid CID, or a valid CID was issued with the wrong ACB, or INTRPRET is being used for a cross-domain LU.

You might have inadvertently modified the field, initially failed to set it, or used the CID of a session that no longer exists.

Another possibility is that you violated the following rule: when placing a CID into the RPLARG field, always use the ARG keyword (ARG=(6), for example), and when placing an NIB address into the RPL's NIB field, always use the NIB keyword (for example, NIB=(6)). Because these two fields occupy the same 4 bytes in the RPL, VTAM can distinguish between an NIB address and a CID only through your use of the ARG or NIB keyword. Thus, the presence of this return code could mean that you placed an NIB address in the RPL with the ARG keyword, and VTAM has rejected your CID as not valid.

This feedback information is also used when a CID is specified for INTRPRET, and the LU implied by the CID is in another domain.

RTNCD	FDB2	Explanation
20(X'14')	30(X'1E')	Data address or length not valid

A request was issued that specified a work area address that is beyond the addressable range of your application program. Here a work area is defined to be any storage area addressed by an RPL operand, for example, the areas referenced by AREA and AAREA.

Check the work area address and work area length fields in the RPL for an incorrect setting. See the RPL macroinstruction description in z/OS Communications Server: SNA Programming to determine which fields must point to valid work areas for each macroinstruction.

If your application program resides in an authorized library, check for correct load module characteristics.

RTNCD	FDB2	Explanation
20(X'14')	35(X'23')	Request type not valid

When an RPL-based macroinstruction is issued, VTAM sets the REQ field in the RPL to indicate the type of macroinstruction that is using the RPL. The presence of this return code indicates that you modified that code before the requested operation completed. To avoid this and other related errors, never modify an RPL while it is in use. Compare with VSAM request, (RTNCD,FDB2)=(X'14',X'00').

RTNCD	FDB2	Explanation
20(X'14')	36(X'24')	Request for address space not valid

You attempted to issue one of the following macroinstructions in other than the session address space: RECEIVE OPTCD=SPEC, RESETSR, SEND, or SESSIONC (except request rejected response to BIND).

RTNCD	FDB2	Explanation
20(X'14')	59(X'3B')	NFME-NRRN response

You attempted to send a response with the RESPOND field set to NFME and NRRN. A response must be identified as FME, RRN, or both; in effect, you have identified the response as neither.

RTNCD	FDB2	Explanation
20(X'14')	60(X'3C')	Previous macroinstruction outstanding

You issued a SEND POST=SCHED, a SEND for an expedited data-flow-control request, or a SESSIONC macroinstruction before a previous macroinstruction of the same type had been completed. Only one macroinstruction of the three preceding types can be outstanding on a session at a time. After the previous macroinstruction has been completed, this macroinstruction can be reissued.

RTNCD	FDB2	Explanation
20(X'14')	64(X'40')	CONTROL not valid

You modified the bits in the CONTROL field, or you used a CONTROL value for a SESSIONC macroinstruction that was not BIND, RQR, SDT, CLEAR, STSN, or SWITCH.

RTNCD	FDB2	Explanation
20(X'14')	65(X'41')	Data traffic not allowed

You attempted to communicate on a session for which no SDT request had been sent or for which a CLEAR is in progress. For certain TS profiles, until an SDT request/response exchange has occurred on the session, no traffic flow is possible; only SDT, Set and Test Sequence Numbers (STSN), Request Recovery (RQR), and Clear requests can be exchanged. Every time a Clear request is sent on a session, a new SDT request might be required before traffic flow can resume (this depends upon the transmission services profile used). For further information, refer to z/OS Communications Server: SNA Programming.

RTNCD	FDB2	Explanation
20(X'14')	66(X'42')	STYPE for SESSIONC not valid

STYPE=RESP has been specified for a SESSIONC CONTROL=CLEAR or a SESSIONC CONTROL=RQR macroinstruction. Only STYPE=REQ is valid. Also, if the NIB used to establish the session specified SDT=SYSTEM, then STYPE=RESP is not valid for SESSIONC CONTROL=SDT.

RTNCD	FDB2	Explanation
20(X'14')	68(X'44')	RESPLIM exceeded

The number of outstanding SEND POST=RESP macroinstructions for a session exceeds the RESPLIM value set in the NIB used to establish the session.

RTNCD	FDB2	Explanation
20(X'14')	71(X'47')	3270 SEND option not valid

The RPL specified by your LU type 0 3270 SEND macroinstruction had one or more of the following fields not valid: STYPE, RESPOND, CHAIN, or CONTROL. See z/OS Communications Server: SNA Programming for more information about exception conditions.

If the RPL was last used for a RECEIVE for the 3270, check the RESPOND field first; you might have failed to reset the field following the RECEIVE (RECEIVE sets the RESPOND field to (NEX,NFME,NRRN) in this case).

RTNCD	FDB2	Explanation
20(X'14')	72(X'48')	Session-control protocol violation

Protocol violations indicated are as follows:

- The PLU sent an SDT request while not in data-traffic-reset state, or the SDT sent was not allowed by the TS profile.
- The PLU sent a Clear request, and a previous Clear request has been sent and has not completed, or the Clear request was not allowed by the TS profile.
- The PLU sent an STSN request while not in data-traffic-reset state, or the STSN request was not allowed by the TS profile.
- The PLU sent an RQR request, and the RQR request was not allowed by the TS profile.
- The SLU sent an SDT response and any previously received SDT request had already been responded to, or an SDT request had not been received.

For more information, refer to z/OS Communications Server: SNA Programming.

RTNCD	FDB2	Explanation
20(X'14')	73(X'49')	STSN action/result code not valid

One of the following situations applies:

- You attempted to send a Set and Test Sequence Numbers (STSN) request and set the IBSQAC or OBSQAC fields (or both) to some value other than SET, TESTSET, IGNORE, or INVALID.
- You attempted to send an STSN response and set the IBSQAC or OBSQAC field (or both), to some value other than TESTPOS, TESTNEG, INVALID, or RESET.
- You attempted to send a result code that is not a valid response to the action code.

Refer to z/OS Communications Server: SNA Programming for more information.

RTNCD	FDB2	Explanation
20(X'14')	74(X'4A')	Installation-wide exit routine was not available

You issued an INTRPRET macroinstruction; VTAM has located the appropriate entry in the interpret table, and found that the system programmer has specified a logon-interpret exit routine to do the interpret function. That routine, however, has not been loaded.

RTNCD	FDB2	Explanation
20(X'14')	75(X'4B')	INTRPRET sequence or LOGMODE not valid, or cryptographic incompatibility

You issued an INTRPRET macroinstruction. One of the following situations might apply:

- VTAM cannot locate an entry in the interpret table that corresponds to the sequence you provided.
- You might have inadvertently modified the sequence or the address in the RPL's AREA field that points to the sequence.
- The system programmer might have failed to properly define the entry in the interpret table.

After your application program has been tested and debugged and you have eliminated the possibility of the three situations listed above, you can assume that the terminal operator or program that initiated the logon must have passed an invalid logon sequence to your application program.

You issued an INQUIRE, OPNDST, SIMLOGON, REQSESS, or CLSDST OPTCD=PASS macroinstruction. Either the NIB for this request specified a logon mode name that could not be found in the logon mode table for the logical unit named in that NIB, or the SSCP discovered that cryptography had been specified for the requested session, but at least one of the logical units in the requested session did not support cryptography.

RTNCD	FDB2	Explanation
20(X'14')	76(X'4C')	Search argument for INQUIRE or INTRPRET not valid

You issued INQUIRE or INTRPRET, and failed to properly provide VTAM with the identity of the pending active session, logical unit, or application program:

- INTRPRET was issued and the name in the NIB was not that of a logical unit.
- INQUIRE (OPTCD=APPSTAT) was issued and one of the following conditions exists:
  - The name is not that of an application program.
  - The application program is a cross-domain resource, and the SSCP that owns the resource does not support INQUIRE (OPTCD=APPSTAT).
  - The application program is a cross-domain resource, and no active route exists to the host that owns the application program.
- INQUIRE OPTCD=TERMS was issued and the name was not that of a resource (such as an LU, PU, CLUSTER, or CDRSC) in the VTAM configuration tables.
- INQUIRE OPTCD=DEVCHAR was issued and the device characteristics were not available (perhaps because the logical unit was in another domain and there was no appropriate CINIT queued for the application program).
- INQUIRE OPTCD=LOGONMSG was issued and there was no appropriate CINIT queued for the application program.
- INQUIRE OPTCD=SESSPARM was issued with LOGMODE=0 in the NIB, and there was no appropriate CINIT queued for the application program.
- INQUIRE OPTCD=NQN was issued and one of the following situations applies:
  - The resource does not exist.
  - The resource is cross-domain an there is no active route to it.

Refer to z/OS Communications Server: SNA Programming for a description of the INQUIRE macroinstruction.

Assuming that the system programmer properly defined the entry in the VTAM configuration tables for the logical unit, you have probably: (1) failed to set a valid symbolic name in the NIB's NAME field or (2) correctly issued INQUIRE OPTCD=SESSPARM or INQUIRE OPTCD=DEVCHAR but the session has been terminated.

RTNCD	FDB2	Explanation
20(X'14')	77(X'4D')	No interpret table

You issued an INTRPRET macroinstruction, but there is no interpret table for the logical unit. The system programmer might have failed to include an interpret table for this logical unit during the VTAM definition process or the logical unit might be in another domain.

RTNCD	FDB2	Explanation
20(X'14')	78(X'4E')	Use of an NIB list not valid

You issued OPNDST OPTCD=ACCEPT without setting the NIB's LISTEND field to YES, or you specified a NIB list in which more than one NIB indicated PROC=NEGBIND.

RTNCD	FDB2	Explanation
20(X'14')	79(X'4F')	OPTCD setting not valid

The OPNDST or INQUIRE request fails because bits in the OPTCD field have been incorrectly set. From the OPNDST and the INQUIRE option code settings, you must specify only one value for the mutually exclusive sets of option codes. Because you cannot cause the field to be incorrectly set by using VTAM macroinstructions, you might have inadvertently modified the OPTCD field with assembler instructions.

RTNCD	FDB2	Explanation
20(X'14')	80(X'50')	RPL field not valid

The OPNDST, CLSDST, SIMLOGON, or REQSESS failed because the bits in the RPL's OPTCD or AAREA field were found to be not valid.

If an OPNDST or SIMLOGON failed, the particular bits that have been incorrectly set are those that form the CONANY-CONALL option code. This return code does not mean that the CONANY option was erroneously used in place of CONALL, or vice versa; it means that neither CONALL nor CONANY is indicated in the OPTCD field. Because you cannot cause the field to be incorrectly set in this manner by using VTAM macroinstructions, you might have inadvertently modified the OPTCD field with assembler instructions.

If a REQSESS failed, either OPTCD=NQ was not specified or the AAREA field of the RPL was not set to zero.

If a CLSDST failed, OPTCD=SENSE was specified and a zero sense was provided in the SSENSEO, SSENSMO, USENSEO fields of the RPL. A zero sense is not permitted for CLSDST OPTCD=SENSE.

RTNCD	FDB2	Explanation
20(X'14')	81(X'51')	OPNDST OPTCD=ACCEPT and SIMLOGON not allowed

You attempted to issue OPNDST OPTCD=ACCEPT to accept a CINIT for a session with a logical unit, or to issue SIMLOGON to initiate a session. However, these operations cannot be performed because of one of the following reasons:

- The ACB was opened with MACRF=NLOGON.
- SETLOGON OPTCD=QUIESCE was issued and CINITs are pending.
- SETLOGON OPTCD=QUIESCE was issued and no matching CINIT was found.

RTNCD	FDB2	Explanation
20(X'14')	82(X'52')	NIB not valid

The request failed because there is no NIB at the location indicated in the RPL's NIB field.

RTNCD	FDB2	Explanation
20(X'14')	83(X'53')	Logical unit not found

The symbolic name you supplied in the NIB's NAME field or indicated by the RPL's AAREA field does not have a corresponding entry in the VTAM configuration tables. This can occur for one of the following reasons:

- You failed to set the NAME field correctly.
- The system programmer did not include the entry in the VTAM configuration tables during VTAM definition.
- The VTAM operator has not activated the major node containing the application program that issued the macroinstruction.
- The VTAM operator has not activated the major node containing the resource named in the NIB (in a cross-domain environment).
- A dynamically created definition for a cross-domain LU has been deleted after lack of use for a defined period of time.
- Contact with the resource was lost and the definition of the resource was subsequently deleted from the VTAM configuration tables.
- You issued either SETLOGON OPTCD=GNAMEADD, SETLOGON OPTCD=GNAMESUB, SETLOGON OPTCD=GNAMEDEL, INQUIRE OPTCD=SESSNAME, or CHANGE OPTCD=ENDAFFIN and one of the names you supplied is not valid.

If you were using an NIB list, no sessions have been established.

RTNCD	FDB2	Explanation
20(X'14')	85(X'55')	One of the following situations is true: • Application program is not authorized. • Application program name is not available. • Task association is not specified. • Application is not authorized to supply dial parameters. • PU is not authorized to accept dial parameters. • You must issue a send RPL.

- You attempted to acquire a logical unit (SIMLOGON or OPNDST), but the installation has denied you authorization to do so. The system programmer might have specified during VTAM definition that your application program is not authorized to acquire any logical units. If you are authorized to acquire logical units and you still receive this return code, this means that an authorization exit routine has been invoked and has determined that you cannot acquire the specific logical unit indicated in your request.
- You attempted to initiate a session, but the authorization exit routine has denied you authorization.
- You issued an INTRPRET macroinstruction; VTAM located the appropriate entry in the interpret table and found that the installation has specified an exit routine to convert the input sequence into an output sequence. That routine was loaded, but it failed to do the conversion.
- You issued one of the following macroinstructions in SRB mode without specifying the required task association: CLSDST, INQUIRE, INTRPRET, OPNDST, OPNSEC, REQSESS, RCVCMD, SENDCMD, SETLOGON, SIMLOGON, TERMSESS.

  Refer to z/OS Communications Server: SNA Programming for more information.
- An application that is not authorized to supply dial parameters attempted to supply dial parameters, or a PU that is not authorized to accept dial parameters attempted to accept dial parameters.

Refer to the z/OS Communications Server: SNA Resource Definition Reference for information about coding an application program major node (the AUTH operand of the APPL definition statement).

RTNCD	FDB2	Explanation
20(X'14')	87(X'57')	MODE field not valid

You issued an OPNDST or OPNSEC macroinstruction and failed to set the NIB's MODE field to RECORD.

RTNCD	FDB2	Explanation
20(X'14')	94(X'5E')	CLSDST OPTCD=PASS not authorized

CLSDST OPTCD=PASS is a function whose use is authorized by the installation. You attempted to use this function, but the installation has not authorized you to pass logical units to other primary logical units. This CLSDST macroinstruction should have been issued with RELEASE in effect, not PASS.

Refer to the z/OS Communications Server: SNA Resource Definition Reference for a description of the AUTH operand of the APPL definition statement.

RTNCD	FDB2	Explanation
20(X'14')	96(X'60')	LU name for CLSDST, SESSIONC, or OPNSEC not valid

You attempted to terminate a session with a logical unit that is not in session with your application program, or had no CINIT queued for your application program. This return code applies to CLSDST used with a logical unit's symbolic name.

You issued a SESSIONC macroinstruction to send a request rejected response to BIND, but the LU name field in the NIB does not match any BIND currently queued for the application program.

You issued an OPNSEC macroinstruction and a queued BIND could not be found for the LU name passed in the NIB.

RTNCD	FDB2	Explanation
20(X'14')	97(X'61')	SETLOGON not valid

Either you opened the ACB with its MACRF field set to NLOGON, or you issued SETLOGON OPTCD=QUIESCE and permanently closed the CINIT queue. Because you attempted to either open a CINIT queue that cannot be opened or close a CINIT queue that is closed, SETLOGON START, STOP, and QUIESCE are not valid.

You might have issued a SETLOGON OPTCD=PERSIST or NPERSIST with a PSTIMER value that is greater than the allowed value (86400 seconds).

Note: You can successfully issue SETLOGON OPTCD=PERSIST or SETLOGON OPTCD=NPERSIST with the MACRF field set to NLOGON or after a QUIESCE.

RTNCD	FDB2	Explanation
20(X'14')	108(X'6C')	Exceeded limit on outstanding RCVCMD requests

You attempted to issue an RCVCMD macroinstruction while a previous RCVCMD was outstanding. The limit on outstanding RCVCMD requests is one.

RTNCD	FDB2	Explanation
20(X'14')	109(X'6D')	Application program not authorized

Your application program is not authorized to issue the SENDCMD and RCVCMD macroinstructions, or your CNM application program attempted to send something other than a formatted Forward RU to the SSCP.

Refer to the z/OS Communications Server: SNA Resource Definition Reference for a description of the AUTH operand of the APPL definition statement.

RTNCD	FDB2	Explanation
20(X'14')	110(X'6E')	Syntax error in reply to VTAM operator message

In reply to a VTAM operator message, you issued a SENDCMD macroinstruction that contained a syntax error in the REPLY command.

RTNCD	FDB2	Explanation
20(X'14')	111(X'6F')	SENDCMD/RCVCMD processor inactive

The portion of VTAM that processes SENDCMD and RCVCMD macroinstructions is currently inactive for your application program, and the application program issued a SENDCMD or RCVCMD macroinstruction. The request cannot be processed because an ACB has not been opened for the portion of the application program that issued the SENDCMD or RCVCMD, or because a final CLOSE has been issued for this ACB but has not yet completed.

RTNCD	FDB2	Explanation
20(X'14')	112(X'70')	Program operator closing ACB with requests outstanding

Your application program is in the process of closing its ACB, and you (1) issued a SENDCMD macroinstruction for a command other than REPLY or (2) issued a RCVCMD OPTCD=Q and there were no VTAM messages available to satisfy the request.

RTNCD	FDB2	Explanation
20(X'14')	113(X'71')	Operator command not valid

You attempted to send a VTAM operator command to VTAM using the SENDCMD macroinstruction; however, the command was not recognized by VTAM, or it was a command (START or HALT) that cannot be sent by the application program.

RTNCD	FDB2	Explanation
20(X'14')	115(X'73')	SEND parameters for CNM not valid

You issued a SEND macroinstruction when using a CNM application program and you have specified a parameter that is not valid.

RTNCD	FDB2	Explanation
20(X'14')	116(X'74')	Negotiable response to non-negotiable BIND

You attempted to issue an OPNSEC PROC=NEGBIND to a non-negotiable BIND request. A request-rejected response to the BIND is sent with a sense code indicating resource unavailable (X'08010000').

RTNCD	FDB2	Explanation
20(X'14')	117(X'75')	Negotiable BIND response parameters not valid

You specified negotiable BIND parameters on an OPNSEC macroinstruction that are not valid. A request rejected response to the BIND is sent with a sense code indicating resource unavailable (X'0801000').

RTNCD	FDB2	Explanation
20(X'14')	118(X'76')	Negotiable BIND response size not valid

You specified a negotiable BIND response on OPNSEC that was greater than 256 bytes. A request rejected response to the BIND is sent with a sense code indicating resource unavailable (X'08010000').

RTNCD	FDB2	Explanation
20(X'14')	119(X'77')	FMD request unit required

You issued a SEND OPTCD=BUFFLST or a SEND OPTCD=LMPEO and the RU specified was not an FMD request unit.

RTNCD	FDB2	Explanation
20(X'14')	120(X'78')	Chain specification not valid

You issued a SEND OPTCD=(BUFFLST,USERRH) in which multiple chains or multiple partial chains were specified in the buffer list. Only requests from a single chain might be specified in a buffer list.

RTNCD	FDB2	Explanation
20(X'14')	121(X'79')	Buffer list length not valid

You issued a SEND OPTCD=BUFFLST, and RECLEN did not contain a nonzero multiple of 16.

RTNCD	FDB2	Explanation
20(X'14')	123(X'7B')	User RH not valid

One of the following conditions was detected for a SEND OPTCD=USERRH:

- The settings of the CONTROL operand and of the RU category field in the user RH were inconsistent. If CONTROL=DATA, then the RU category must be FMD. If CONTROL is not DATA, then the RU category must be DFC. See also (RTNCD,FDB2)=(X'14',X'77').
- A sense indicator in the user RH field was found to be on with zero sense provided. For a non LUO session, zero sense is architecturally incorrect.

RTNCD	FDB2	Explanation
20(X'14')	124(X'7C')	OPTCD=USERRH for SESSIONC not valid

You specified a SESSIONC macroinstruction with OPTCD=USERRH.

RTNCD	FDB2	Explanation
20(X'14')	125(X'7D')	XRF protocol error

A protocol error has occurred during the processing of a SIMLOGON or OPNDST macroinstruction.

SIMLOGON for a backup XRF request is processed by setting the "backup XRF session request" indicator in the INITIATE RU. This indicator is set based on the setting of the RPL bit indicating OPTCD=BACKUP (RPLBCKUP). If an Initiate is received specifying a backup XRF session and queue, it is rejected.

The RPL system-sense (SSENSEI), the system-sense modifier (SSENSMI), and the user-sense (USENSEI) can contain a more detailed explanation of the failure.

RTNCD	FDB2	Explanation
20(X'14')	126(X'7E')	Conflicting OPTCD on a macroinstruction request

One of the following conditions was detected:

- A TERMSESS macroinstruction has been issued with none or more than one of the following OPTCDs specified: COND, UNCOND, and UNBIND.
- A SETLOGON request has been issued with none or more than one of the following OPTCDs specified: HOLD, NPERSIST, PERSIST, QUIESCE, GNAMEADD, GNAMEDEL, GNAMESUB, START, and STOP.
- A SIMLOGON request has been issued with more than one of the following OPTCDs specified: QALL, QSESSLIM, and QNOTENAB.

RTNCD	FDB2	Explanation
20(X'14')	127(X'7F')	Policing error - non-APPC macroinstruction

An application program issued a non-APPCCMD macroinstruction to establish an LU 6.2 session, or issued a non-APPCCMD macroinstruction against a current LU 6.2 session.

RTNCD	FDB2	Explanation
20(X'14')	128(X'80')	SETLOGON not valid

You specified SETLOGON OPTCD=NPERSIST or PERSIST for an application that is not capable of persistence.

RTNCD	FDB2	Explanation
20(X'14')	129(X'81')	TERMSESS without OPTCD=UNBIND with session in a pending state

A TERMSESS macroinstruction is issued for a pending active session without specifying OPTCD=UNBIND.

RTNCD	FDB2	Explanation
20(X'14')	130(X'82')	Parameter length not valid

The length of an application-supplied dial parameter is not valid. Refer to z/OS Communications Server: SNA Programming for a description of the valid lengths.

RTNCD	FDB2	Explanation
20(X'14')	131(X'83')	Subfield error

Either a subfield is not supported, or a combination of subfields that is not valid is specified. Refer to z/OS Communications Server: SNA Programming for information about the valid subfields that can be specified.

RTNCD	FDB2	Explanation
20(X'14')	132(X'84')	NIBASDPA = 0

The value of NIBASDPA is 0. The NIBASDP indicator was on, indicating that the application is providing dial parameters; however, no address for the control block was given. This probably resulted from the application program passing an address that is not valid to the NIB.

RTNCD	FDB2	Explanation
20(X'14')	133(X'85')	Session must be restored

A SEND, RECEIVE, RESETSR, or SESSIONC request is rejected because it is issued for a session that is pending recovery. Use OPNDST OPTCD=RESTORE to restore the session and reissue the request.

RTNCD	FDB2	Explanation
20(X'14')	134(X'86')	Existing session prevents successful completion of this operation

One of the following situations applies:

- You issued CHANGE OPTCD=ENDAFFIN to terminate the association between your application program and the specified LU. At least one session exists between the specified LU and the application program; all sessions with the partner LU must be ended before the association can be terminated.

- You issued SETLOGON OPTCD=GNAMEADD to register your application as a generic resource, but a session exists already.

RTNCD	FDB2	Explanation
20(X'14')	135(X'87')	Resource name and generic name are the same

You attempted to issue either SETLOGON OPTCD=GNAMEADD, SETLOGON OPTCD=GNAMESUB, or SETLOGON OPTCD=GNAMEDEL using a generic name that was the same as the application network name; they must be different.

RTNCD	FDB2	Explanation
20(X'14')	136(X'88')	No association matching the given criteria exists.

You issued either CHANGE OPTCD=ENDAFFIN or INQUIRE OPTCD=SESSNAME, but the values specified in the NIB do not correspond to any known association.

RTNCD	FDB2	Explanation
20(X'14')	137(X'89')	Generic name not authorized

The generic name has not been authorized using a security management product such as RACF.

RTNCD	FDB2	Explanation
20(X'14')	138(X'8A')	Application program already registered

The application program is registered already as a generic resource, but with a different name.

RTNCD	FDB2	Explanation
20(X'14')	139(X'8B')	SETLOGON OPTCD=GNAMEDEL not valid

You used SETLOGON OPTCD=GNAMEDEL to deregister generic resources but VTAM determined that generic mapping does not exist; no VTAM message is issued.

RTNCD	FDB2	Explanation
20(X'14')	140(X'8C')	Network identifiers conflict for this generic resource.

This generic resource exists already with another network identifier.

RTNCD	FDB2	Explanation
20(X'14')	141(X'8D')	Simultaneous generic resource registration in progress

Two applications with the same application network name are simultaneously attempting to register a generic name.

RTNCD	FDB2	Explanation
20(X'14')	142(X'8E')	APPC capabilities conflict

All applications registering as generic resources must have the same APPC capabilities specified on their APPL statements.

RTNCD	FDB2	Explanation
20(X'14')	143(X'8F')	Deletion of VTAM affinity rejected

VTAM owns the affinity. Your application cannot delete it.

RTNCD	FDB2	Explanation
20(X'14')	144(X'90')	USERVAR conflict while registering generic resources

You issued SETLOGON OPTCD=GNAMEADD to register generic resources. VTAM detected a conflict (the generic resource exists already as a USERVAR name).

RTNCD	FDB2	Explanation
20(X'14')	145(X'91')	TSO GENERIC NAME CONFLICT

Either a non-TSO application is attempting to use the generic name already being used by TSO, or TSO is attempting to use the generic name already being used by a non-TSO application.

RTNCD	FDB2	Explanation
20(X'14')	146(X'92')	SETLOGON GNAMESUB FAILURE

A SETLOGON OPTCD=GNAMESUB macroinstruction failed for one of the following reasons:

- SETLOGON OPTCD=GNAMEADD was previously issued for this ACB.
- SETLOGON OPTCD=GNAMESUB was previously issued for this ACB.
- The application program network name specified in the VTAM node identification block (NIB) either was not found or was not an instance of the generic name specified in the NIB.

RTNCD	FDB2	Explanation
20(X'14')	147(X'93')	STOKEN not valid.

PROC=STOKEN is specified and the NIBSTKN field contains an invalid STOKEN.

RTNCD	FDB2	Explanation
20(X'14')	148(X'94')	No LU name passed.

No LU name was passed on the SETLOGON OPTCD=START or on the REQSESS.

RTNCD	FDB2	Explanation
20(X'14')	149(X'95')	No applicable RDTE found.

No RDTE was found that matched the LU name passed on the SETLOGON OPTCD=START or on the REQSESS.

RTNCD	FDB2	Explanation
20(X'14')	150(X'96')	Conflict with found RDTE.

An RDTE was found that matched the LU name passed on the SETLOGON OPTCD=START or on the REQSESS, but its characteristics or state was not appropriate.

RTNCD and FDB2 information for LU 6.2

While most of the LU 6.2 feedback information from errors is found in the RCPRI and RCSEC fields, some error return codes in the RPL RTNCD and FDB2 fields are meaningful for LU 6.2 applications. The X'00', X'0B' combination in the RPL indicates some problem might have occurred while the macro was executing. RCPRI and RCSEC should be used for further diagnosis. The other RTNCD, FDB2 combinations see attempts to start an LU 6.2 session independent of VTAM or attempts to use non-APPCCMD macros for APPCCMD functions. The following table shows the relevant codes.

RTNCD	FDB2	ISTUSFBC EQU label	Meaning
X'00'	X'0B'	USF6APPC	CONDITIONAL COMPLETION FOR APPCCMD

Some type of error might have occurred on an APPCCMD macro. For further problem determination, see the primary and secondary return codes in the RPL extension. These fields are RPL6RCPR and RPL6RCSC.

RTNCD	FDB2	ISTUSFBC EQU label	Meaning
X'04'	X'05'	USFNQN	SYMBOLIC NAME KNOWN BY NETWORK-QUALIFIED NAME ONLY

A real-to-symbolic translation request is made, and NIBNET is filled in with a network identifier, but VTAM cannot provide a symbolic name. VTAM knows this resource only by its network-qualified name. No symbolic name represents this resource. Do one of the following actions:

- Use the network-qualified name.
- Define a symbolic name to represent this resource.

RTNCD	FDB2	ISTUSFBC EQU label	Meaning
X'10'	X'13'	USF6APRJ	ATTEMPT TO START 6.2 SESSION: REQUEST REJECTED

An LU 6.2 application program has tried to start an LU 6.2 session independent of VTAM. No pending sessions have been disturbed. This occurs when an OPNDST is issued with an LU 6.2 user-specified BIND.

RTNCD	FDB2	ISTUSFBC EQU label	Meaning
X'10'	X'14'	USF6APST	ATTEMPT TO START 6.2 SESSION: PENDING SESSION TERMINATED

An LU 6.2 application program has tried to start an LU 6.2 session independent of VTAM. The pending session has been terminated. This occurs when the LOGMODE specified on an OPNDST resolves to an LU 6.2 BIND or when OPNSEC is issued for an LU 6.2 BIND.

RTNCD	FDB2	ISTUSFBC EQU label	Meaning
X'10'	X'15'	USF6APIS	AN APPCCMD MUST BE ISSUED

An OPNDST or CLSDST has been issued for a pending LU 6.2 session. An APPCCMD CONTROL=OPRCNTL, QUALIFY=ACTSESS or QUALIFY=DACTSESS macro must be issued for this session.

RTNCD	FDB2	ISTUSFBC EQU label	Meaning
X'14'	X'7F'	USF6PENA	POLICING ERROR — NON-APPC MACRO

An application program issued a non-APPCCMD macro to establish an LU 6.2 session, or issued a non-APPCCMD macro against a current LU 6.2 session.

RCPRI and RCSEC return codes for LU 6.2

VTAM passes feedback return codes to the LU 6.2 application program in a variety of ways. The principal feedback mechanism is the RCPRI and RCSEC return code fields in the RPL extension. These fields have meaning only when Register 15 is set to X'00' and Register 0 is set to X'0B'. These values are also the values of the RPL RTNCD and FDB2 fields, respectively.

For a general discussion of how register contents relate to RPL feedback fields, see z/OS Communications Server: SNA Programmer's LU 6.2 Guide.

The RPL extension contains two fields in which return code information is passed to the application program at the completion of an APPCCMD macroinstruction execution. The two fields are RPL6RCPRI and RPL6RCSEC, and together they indicate the result of the macroinstruction execution, including any state changes to the specified conversation. The RCPRI field returns a primary return code to the application; the RCSEC field returns a secondary return code to the application. Some RCPRI codes do not have associated RCSEC subcodes. For these RCPRI codes, the RCSEC field is set to X'0000'.

Some of the (RCPRI, RCSEC) return codes indicate the results of the local VTAM's processing of the macroinstruction; these return codes are returned on the APPCCMD that invoked the local processing. Other (RCPRI, RCSEC) return codes indicate the results of processing invoked at the remote end of the conversation and, depending upon the CONTROL and QUALIFY settings of the APPCCMD, can be returned on the APPCCMD that invoked the remote processing or on a subsequent APPCCMD. Still other return codes report events that originate at the remote end of the conversation.

The RCPRI and RCSEC codes are described below. Each description includes the meaning of the code, the reason for the condition indicated by the code, when the code can be reported to the application program, and the state of the conversation (if applicable) when the function of the APPCCMD completes. Actions taken by the local application program are discussed in the following return code descriptions in terms of APPCCMD macroinstructions; actions taken by the remote LU or transaction program are described more generically using the architected protocol boundary verbs documented in the LU 6.2 architecture.

Note: Some application programs change the hexadecimal values from the RCPRI, RCSEC fields to decimal values. You might need to convert these back to hexadecimal values for problem determination.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	(all)	USF6OK	OK

The local application program issued an APPCCMD macroinstruction that executed without error. The function defined for the APPCCMD was performed as specified.

The OK RCPRI code together with one of the following RCSEC subcodes form the complete return code that is returned to the application; the RCSEC subcode provides additional information.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0000'	USF6OKSC	OK

The APPCCMD completed successfully and no additional information is defined for the APPCCMD. If a conversation-related macroinstruction is issued, the conversation state can be found in the CONSTATE field. Whenever this RCPRI,RCSEC combination is present, registers 15 and 0 are also set to 0.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0001'	USF6ASSP	AS SPECIFIED

The CNOS values supplied by the application program on the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction were accepted by the partner LU as specified, without negotiation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0002'	USF6ASNG	AS NEGOTIATED

One or more of the CNOS values supplied by the application program on the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was changed by negotiation with the partner LU. The values are returned to the application program on the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction. (The macroinstruction description defines which values can be negotiated.)

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0003'	USF6RCVR	RECEIVE SPECIFIC REJECTED

An APPCCMD CONTROL=RECEIVE, QUALIFY=SPEC or APPCCMD CONTROL=RECEIVE, QUALIFY=ISPEC macroinstruction was rejected because an APPCCMD CONTROL=RECEIVE, QUALIFY=ANY or APPCCMD CONTROL=RECEIVE, QUALIFY=IANY macroinstruction is currently being processed on this conversation. There is no state change.

See the z/OS Communications Server: SNA Programmer's LU 6.2 Guide for more information on the APPCCMD CONTROL=RECEIVE, QUALIFY=SPEC|ISPEC and APPCCMD CONTROL=RECEIVE, QUALIFY=ANY|IANY macroinstructions.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0004'	USF6SNGL	PARTNER LU SUPPORTS SINGLE SESSION

VTAM has determined that the partner LU supports only single sessions. If the session limit you specified was greater than 1, or if you did not specify a session limit, then the default values of 1, 0, 0 were used for your CNOS request.

If the partner LU indicated single-session capability using a negative BIND response, the partner LU's name will be missing from the Userdata subfield of the BIND. When the application program issues an APPCCMD CONTROL=OPRCNTL, QUALIFY=DISPLAY macroinstruction, it should verify the presence of the partner LU's fully qualified name. If the FQNLEN field is 0, the partner LU's name is not available. Check the FQNLEN field before checking the FQNAME field.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0005'	USF6INER	INTERNAL VTAM ERROR

VTAM rejected the APPCCMD CONTROL=REJECT, QUALIFY=SESSION macroinstruction because of an internal error other than a storage shortage condition.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0006'	USF6RSUN	RESTORE_UNNECESSARY—NO_MODES_TO_RESTORE

The APPCCMD CONTROL=OPRCNTL,QUALIFY=RESTORE macroinstruction is unnecessary. The associated mode (or modes) has been restored already, or nothing existed to restore.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0007'	USF6RSIN	RESTORE_INCOMPLETE—INPUT_WORK_AREA _TOO_SMALL

The APPCCMD CONTROL=OPRCNTL,QUALIFY=RESTORE macroinstruction is incomplete. The AREA supplied is too small to hold all the information that needs to be returned. Reissue the macroinstruction one or more times to obtain all the restore information and to complete the restore.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0008'	USF6NINA	NO IMMEDIATELY AVAILABLE INFORMATION

An APPCCMD that requested the immediate return of available information was issued. However, no information that could satisfy the request was available.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'0009'	USF6RTEC	REQUEST TERMINATED BY END OF CONVERSATION

An APPCCMD was awaiting processing or awaiting the arrival of information or a response on a specific conversation. The command has terminated because the conversation ended before the requested information became available or before it could be processed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'000A'	USF6ANMS	SESSIONS WILL USE APPL NAME, GENERIC NAME REQUESTED

Use of the generic resource name was requested but the application network name is required.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'000B'	USF6GNMS	SESSIONS WILL USE GENERIC NAME, APPL NAME WAS REQUESTED

Use of the application network name was requested but the generic resource name is required.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'000C'	USF6NAM1	AS SPECIFIED, PARTNER LU KNOWN BY DIFFERENT NAME

The CNOS values supplied by the application program on the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction were acceptable by the partner LU as specified, without negotiation. Furthermore, the CNOS operation caused an LU entry of type RCVD_NAME to be changed to a VARIANT_NAME entry in the LU-mode table.

For more information, see the z/OS Communications Server: SNA Programmer's LU 6.2 Guide.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0000'	X'000D'	USF6NAM2	AS NEGOTIATED, PARTNER LU KNOWN BY DIFFERENT NAME

One or more of the CNOS values supplied by the application program on the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was changed by negotiation with the partner LU. The values are returned to the application program on the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction. (The macroinstruction description defines which values can be negotiated.) Furthermore, the CNOS operation caused an LU entry of type RCVD_NAME to be changed to a VARIANT_NAME entry in the LU-mode table.

For more information, see the z/OS Communications Server: SNA Programmer's LU 6.2 Guide.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	(all)	USF6ALLC	ALLOCATION ERROR

The application program issued APPCCMD CONTROL=ALLOC and allocation of the specified conversation could not be completed. When the ALLOCATION_ERROR RCPRI code is used with one of the following RCSEC subcodes (X'0000'–X'000F'), they form the complete return code that is returned to the program. The RCSEC subcode identifies the specific error. (The partner LU and remote transaction program referred to in the following RCSEC definitions are the LU named in the LUNAME field of the APPCCMD, and the transaction program named in the FMH-5 supplied through the AREA field of the APPCCMD, respectively.)

If the partner LU detects the error that causes an ALLOCATION_ERROR RCPRI code to be returned to the application, the error indicator sent by the partner LU can specify that error log data follows the error indicator. The error log data indicator is returned to the application program in the LOGRCV field of the completed macroinstruction. If an ALLOCATION_ERROR RCPRI code is returned to the application along with LOGRCV=YES, the conversation should issue APPCCMD CONTROL=RECEIVE, QUALIFY=SPEC to receive the error log data. When the error log data is received, the conversation is over.

If an ALLOCATION_ERROR RCPRI code is returned to the application along with LOGRCV=NO, the conversation is in END_CONV state.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0000'	USF6ALNR	ALLOCATION FAILURE NO RETRY

The conversation cannot be allocated on a session because of a permanent condition. For example, the session to be used for the conversation cannot be activated for one of the following reasons:

- The mode is closed; the current session limit is 0.
  - CNOS has not been negotiated and no entry has been created for the mode.
  - A previous CNOS request has set limits to 0.
- A system definition error.
- A session-activation protocol error.

The session also might be deactivated because of a session protocol error before the conversation could be allocated. The application program should not try the allocation request again until the condition is corrected. The application should check the returned SENSE field in the RPL extension for an indication of the exact error.

If this code occurs when issuing a DISPLAY APING operator command, the session might have been deactivated as a result of processing a received APING request for the same mode. Reissue the operator command.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0001'	USF6ALR	ALLOCATION FAILURE RETRY

The conversation cannot be allocated on a session because of a temporary condition. For example, the session to be used for the conversation cannot be activated because of a temporary lack of resources at the remote LU; or the session was deactivated because of session outage before the conversation could be allocated. The condition is temporary, and the program can try the allocation request again.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0002'	USF6ALCM	CONVERSATION TYPE MISMATCH

The partner LU rejected the allocation request because the remote transaction program does not support the respective mapped or basic protocol boundary. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0003'	USF6ALPI	PIP NOT ALLOWED

The partner LU rejected the allocation request because the local application program provided program initialization parameter (PIP) data (along with the FMH-5) and either the partner LU does not support PIP data, or the remote transaction program has no PIP variables defined. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0004'	USF6ALPP	PIP NOT SPECIFIED CORRECTLY

The partner LU rejected the allocation request because the remote transaction program has one or more PIP variables defined and the local application program provided no program initialization parameters, or the local application program specified program initialization parameters (along with the FMH-5) that do not correspond in number to those defined for the remote transaction program. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0005'	USF6ALSC	SECURITY NOT VALID

The partner LU rejected the allocation request because the access security information supplied by the local application (in the FMH-5) is not valid. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0006'	USF6ALSY	SYNC LEVEL NOT SUPPORTED BY LU

The partner LU rejected the allocation request because the synchronization level specified in the allocation request is not supported by both the local and partner LU. The local LU specifies its level of synchronization support on its APPL statement. The partner LU has returned the negotiated level between the two LUs in the BIND response. This return code is returned on the APPCCMD CONTROL=ALLOC macroinstruction for the local LU.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0007'	USF6ALSL	SYNC LEVEL NOT SUPPORTED BY PROGRAM

The partner LU rejected the allocation request because the local application program specified a synchronization level (in the FMH-5) that the remote transaction program does not support. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0008'	USF6ALTP	TPN NOT RECOGNIZED

The partner LU rejected the allocation request because the local application program specified a remote transaction program name (TPN) that the partner LU does not recognize. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0009'	USF6ALTN	TRANSACTION PROGRAM NOT AVAILABLE, NO RETRY

The partner LU rejected the allocation request because the local application program specified a remote transaction program that the partner LU recognizes but cannot start. The condition is not temporary, and the application should not try the allocation request again. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'000A'	USF6ALTR	TRANSACTION PROGRAM NOT AVAILABLE, RETRY

The partner LU rejected the allocation request because the local application specified a remote program that the remote LU recognizes but currently cannot start. The condition is temporary, and the application can try the allocation request again. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'000B'	USF6ALRN	CANNOT RECONNECT TRANSACTION PROGRAM, NO RETRY

The partner LU rejected the reconnection request because it does not recognize the conversation correlator. The condition is not temporary, and the application should not try the reconnection request again. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'000C'	USF6ALRR	CANNOT RECONNECT TRANSACTION PROGRAM, RETRY

The partner LU rejected the reconnection request because it currently cannot reconnect the remote transaction program implied by the conversation correlator. The condition is temporary, however, and

the application can try the reconnection request again. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'000D'	USF6ALNS	RECONNECT NOT SUPPORTED BY PROGRAM

The partner LU rejected the allocation request because the local application program specified a recovery level of program reconnect (in the FMH-5) and the remote transaction program does not support program reconnect. This return code is returned on an APPCCMD subsequent to APPCCMD CONTROL=ALLOC.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'000E'	USF6SPMA	MODE MUST BE RESTORED BEFORE USING

The APPCCMD CONTROL=ALLOC macroinstruction is rejected because the specified mode name is pending recovery for persistent LU-LU sessions. Restore the mode by issuing APPCCMD CONTROL=OPRCNTL, QUALIFY=RESTORE.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'000F'	USF6DARQ	DEALLOCATION REQUESTED

The allocation request has been cancelled before its normal processing could be completed. The local application program issued a request for abnormal deallocation of the pending conversation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0010'	USF6ALSF	ALLOCATION ERROR - SYNCH LEVEL NOT VALID FOR FULL-DUPLEX

The allocation request has been rejected because it specifies a full-duplex conversation with a sync point level not allowed for a full-duplex conversation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0004'	X'0011'	USF6LNSF	ALLOCATION ERROR - LU PAIR NOT SUPPORTING FDX CONVERSATION

The allocation request has been rejected because it specifies a full-duplex conversation and the negotiated level of support between the local application and the partner LU does not allow full-duplex conversations.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	(all)	USF6CNSA	CNOS FAILURE

The APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction did not process successfully. The CNOS_ALLOCATION_ERROR RCPRI code together with one of the following RCSEC subcodes (X'0000'–X'0006') form the complete return code that is returned to the transaction program. The RCSEC subcode identifies the specific error. The local and partner LUs' CNOS parameters are not changed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0000'	USF6CANR	ALLOCATION FAILURE NO RETRY

The control operator conversation cannot be allocated because of a condition that is not temporary. For example, the session to be used for the control operator conversation cannot be activated because the session limit for the specified partner LU and SNASVCMG mode name is currently 0 at either the local LU or partner LU; or because of a system definition error or a session-activation protocol error; or because a session protocol error caused the session to be deactivated before the conversation could be allocated. The CNOS will not be able to complete successfully until the condition is corrected. This code can also be returned if a partner LU rejects a SNASVCMG mode name BIND.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0001'	USF6CAR	ALLOCATION FAILURE RETRY

The control operator conversation cannot be allocated because of a temporary condition. For example, the session to be used for the control operator conversation cannot be activated because of a temporary lack of resources at the local LU or partner LU, or the session was deactivated because of session outage before the conversation could be allocated. The condition is temporary, and the control operator can try the transaction again later.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0002'	USF6CATR	TRANSACTION PROGRAM NOT AVAILABLE, RETRY

The partner LU is currently unable to start the transaction program identified as hex 06F1, which is the SNA service transaction program for the control operator. For example, there can be a temporary lack of resources the partner LU needs to start the transaction program. The condition is temporary, and the control operator can try the transaction again later.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0003'	USF6CATN	TRANSACTION PROGRAM NOT AVAILABLE, NO RETRY

The partner LU is unable to start the transaction program identified as X'06F1', which is the SNA service transaction program for the control operator. The condition is not temporary, and the application should not try the CNOS request again.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0004'	USF6CACM	CONVERSATION TYPE MISMATCH

The partner LU rejected the CNOS conversation allocation request because the remote transaction program does not support the respective mapped or basic protocol boundary.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0005'	USF6CASC	SECURITY NOT VALID

The partner LU rejected the CNOS conversation allocation request because the access security information supplied by VTAM (in the FMH-5) is invalid.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0006'	USF6SPMC	MODE MUST BE RESTORED BEFORE USING

The APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction is rejected because the specified mode name is pending recovery for persistent LU-LU sessions. Restore the mode by issuing APPCCMD CONTROL=OPRCNTL, QUALIFY=RESTORE. New modes can be added once the SNASVCMG mode for an LU has been restored, but any mode that exists when the failure (or takeover) occurs cannot be used until that mode has been restored.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0008'	X'0007'	USF6NQNM	NETWORK QUALIFIED NAME MISMATCH

The name on an APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was an ACB name. The ACB name is not identical to the network resource name. ACB names cannot be used in cross-domain, cross-network, or network qualified. For information on coding the ACBNAME operand, see the z/OS Communications Server: SNA Resource Definition Reference.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'000C'	X'0000'	USF6CNSN	CNOS RESOURCE FAILURE, NO RETRY

The APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction did not execute successfully because of a failure that caused the control operator conversation to be deallocated prematurely. For example, the session being used for the control operator conversation was deactivated for one of the following reasons:

- A session protocol error
- A session outage from which the control operator component of the LU could not recover.

The conversation also might be deallocated because of a protocol error between the control operator components of the LUs. The condition is not temporary, and the control operator should not try the transaction again until the condition is corrected. The CNOS parameters remain unchanged at the local LU, or both the local and partner LUs, depending on when the failure occurred.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0010'	(all)	USF6CRRJ	COMMAND RACE REJECT

The APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction did not execute successfully because two CNOS operations caused contention for the needed resources.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0010'	X'0000'	USF6CRPR	PARTNER GRANTED RETRY

Both LUs initiated a CNOS negotiation for the same mode at the same time. The partner LU will try the CNOS request again. VTAM fails the CNOS request from the local LU.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0010'	X'0001'	USF6CRLR	CONTROL OPERATOR FOR LOCAL LU RETRIED

Both LUs initiated CNOS processing for the same mode at the same time. VTAM failed the partner's CNOS attempt, and the local LU was given permission to try the CNOS request again. VTAM attempted CNOS processing again but the subsequent CNOS negotiation failed as well. VTAM was forced to fail the local LU's CNOS request.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0010'	X'0002'	USF6PCIP	PARTNER CNOS IN PROGRESS

The partner LU has already begun processing a CNOS for the same mode name, and its processing will continue uninterrupted. The application program must reissue this APPCCMD for it to be processed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0010'	X'0003'	USF6LPSS	LU IN PENDING SINGLE STATE

The CNOS negotiation cannot be attempted at this time because the partner LU has initiated a CNOS request for the same mode. The partner LU might be a single-session-capable LU. The local LU cannot issue a CNOS request until the CNOS request initiated by the partner LU completes.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0010'	X'0004'	USF6PLSS	PARTNER LU STARTING SESSION

A partner LU that provides only single-session support is currently initiating a session. Because only one session can be active at a time, the application program's CNOS request is rejected. The application program can try the CNOS command again later.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0014'	X'0000'	USF6DABP	DEALLOCATE ABEND PROGRAM

The remote transaction program issued a DEALLOCATE verb, as defined in the LU 6.2 architecture, specifying the TYPE(ABEND_PROG) parameter, or the remote LU did so because of a remote transaction program abend condition. If the conversation for the remote transaction program was in a state in which information can be received when the DEALLOCATE was issued, information sent by the local application and not yet received by the remote transaction program was purged. This return code can be reported to the local application on any APPCCMD macroinstruction that can process the error notification on a half-duplex conversation. This return code can only be reported on an APPCCMD CONTROL=RECEIVE on a full-duplex conversation. The error indicator sent by the partner LU to specify the DEALLOCATE_ABEND_PROGRAM condition can specify that error log data follows the error indicator. The error log data indicator is returned to the application program in the LOGRCV field of the completed macroinstruction. If a DEALLOCATE_ABEND_PROGRAM RCPRI code is returned to the application along with LOGRCV=YES, the conversation should issue APPCCMD CONTROL=RECEIVE, QUALIFY=SPEC|ISPEC to receive the error log data. The conversation is then ended. If a DEALLOCATE_ABEND_PROGRAM RCPRI code is returned to the application along with LOGRCV=NO, the conversation is ended.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0018'	X'0000'	USF6DABS	DEALLOCATE ABEND SERVICE

The remote transaction program issued a DEALLOCATE verb, as described in the LU 6.2 architecture, specifying the TYPE(ABEND_SVC) parameter. If the conversation for the remote transaction program was in a state in which information can be received when the DEALLOCATE was issued, information sent by the local application and not yet received by the remote transaction program was purged. This return code can be reported to the local application on any APPCCMD macroinstruction that can process the error notification on a half-duplex conversation. This return code can only be reported on an APPCCMD CONTROL=RECEIVE on a full-duplex conversation. The error indicator sent by the partner LU to specify the DEALLOCATE_ABEND_SERVICE condition can specify that error log data follows the error indicator. The error log data indicator is returned to the application program in the LOGRCV field of the completed macroinstruction. If a DEALLOCATE_ABEND_SERVICE RCPRI code is returned to the application along with LOGRCV=YES, the conversation is in PEND_END_CONV_LOG or PEND_RESET_LOG state. If a DEALLOCATE_ABEND_SERVICE RCPRI code is returned to the application along with LOGRCV=NO, the conversation is in END_CONV or FDX_RESET state.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'001C'	X'0000'	USF6DABT	DEALLOCATE ABEND TIMER

The remote transaction program issued a DEALLOCATE verb, as described in the LU 6.2 architecture, specifying the TYPE(ABEND_TIMER) parameter. If the conversation for the remote program was in a state in which information can be received when the DEALLOCATE was issued, information sent by the local application program and not yet received by the remote transaction program was purged. This return code can be reported to the local program on any APPCCMD macroinstruction that can process the error notification on a half-duplex conversation. This return code can only be reported on an APPCCMD CONTROL=RECEIVE on a full-duplex conversation. The error indicator sent by the partner LU to specify the DEALLOCATE_ABEND_TIMER condition can specify that error log data follows the error indicator. The error log data indicator is returned to the application program in the LOGRCV field of the completed macroinstruction. If a DEALLOCATE_ABEND_TIMER RCPRI code is returned to the application along with LOGRCV=YES, the conversation is in PEND_END_CONV_LOG or PEND_RESET_LOG state. If a DEALLOCATE_ABEND_TIMER RCPRI code is returned to the application along with LOGRCV=NO, the conversation is in END_CONV or FDX_RESET state.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0020'	X'0000'	USF6CNSR	CNOS FAILURE, RETRY

The APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued and a conversation was begun with the partner LU. However, a failure occurred that caused the conversation to be prematurely terminated. For example, the session being used for the conversation was deactivated because of a session outage, such as a line failure or a modem failure. The condition is temporary, and the application can try the transaction again.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0024'	X'0000'	USF6LRBE	LOGICAL RECORD BOUNDARY ERROR

The application program began sending a logical record before the previous logical record was sent in its entirety. The conversation state does not change.

For macroinstructions that use the QUALIFY=DATACON keyword, the data that was to be sent with the confirmation request is held. The application program must either furnish more data to finish the logical record, or truncate the incomplete record. The application cannot immediately send more data to

complete the logical record, but must explicitly flush the send buffer and then send data to complete the logical record.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0028'	X'0000'	USF6SLCL	LU MODE SESSION LIMIT CLOSED

The APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction did not execute successfully because the partner LU currently will not allow the session limit for the specified mode name to be raised above 0. The session limit remains at 0. This condition is not necessarily permanent; the control operator can try the CNOS transaction again later.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	(all)	USF6PARM	PARAMETER ERROR

VTAM rejected the APPCCMD because one of the RPL, RPL extension, or session limits structure fields specified in the APPCCMD contained a value that was not valid. The PARAMETER_ERROR RCPRI code together with the following RCSEC subcodes (X'0000'–X'002D') form the complete return code that is returned to the application. The subcode identifies the specific error. This RCPRI code is returned on the APPCCMD that contained the parameter that was not valid. When this RCPRI code is returned on a conversation APPCCMD macroinstruction (that is, a macroinstruction that does not specify CONTROL=OPRCNTL), the state of the conversation remains unchanged. When this RCPRI code is returned on an APPCCMD CONTROL=OPRCNTL macroinstruction, the local and partner LUs' CNOS parameters are not changed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0000'	USF6IVLU	INVALID LU NAME OR NETWORK IDENTIFIER

The APPCCMD specified an unrecognized partner LU name or network identifier.

This combination of return codes might result if VTAM does not find the LU name for a partner in the LU-mode table. The partner LU name and the (logon) mode name are added to the dynamically built LU-mode table during CNOS negotiation. To initiate CNOS negotiation, the application program issues the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction and specifies the LU name and logon mode (LOGMODE) name to be used during communication.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0001'	USF6IVMD	INVALID MODE

The APPCCMD specified an unrecognized logmode name, or the logmode name is not allowed for the LU-LU pair.

This combination of return codes might occur if the LU name specified for a conversation allocation request is present in the LU-mode table but the (logon) mode name is not present. The partner LU name and the (logon) mode name are added to the dynamically built LU-mode table during CNOS negotiation. To initiate CNOS negotiation, the application program issues the APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction and specifies the LU name and logon mode (LOGMODE) name to be used during communication.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0002'	USF6IVCI	INVALID CONVERSATION

The APPCCMD specified an unassigned conversation ID, or the RPL used for the request specified an ACB other than the one associated with the conversation assigned that CONVID. The value specified might have been a valid CONVID, but the conversation might not be active.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0003'	USF6IVLL	INVALID LL

The data provided by the application program on an APPCCMD CONTROL=SEND, an APPCCMD CONTROL=PREPRCV, or an APPCCMD CONTROL=DEALLOC macroinstruction contained an invalid logical record length (LL) value of X'0000', X'0001', X'8000', or X'8001'. An LL value of hex 0001, which indicates that the data contains a presentation services (PS) header for sync point, is allowed only on conversations with a synchronization level of sync point.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0004'	USF6IVSV	INVALID VALUES FOR SNASVCMG MODE

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued and the values specified for the SESSLIM, MINWINL, and MINWINR do not specify (2,1,1) or (0,0,0), respectively.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0005'	USF6IVDL	INVALID DRAINL CHANGE

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued, NBRMODE=ONE and DRAINL=YES were specified, the session limit in effect when the APPCCMD was issued was 0, and DRAINL=NO was in effect when the APPCCMD was issued. (The application program attempted to change DRAINL from NO to YES on an APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction when session limits were 0.)

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0006'	USF6SNAR	SNASVCMG MODE CANNOT CURRENTLY BE RESET

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction is issued, the SNASVCMG mode name is specified, and either one or more session limits for the mode name group for the partner LU is not 0; or one or more session limits for the mode name group for the partner LU is 0, but draining is enabled.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0007'	USF6MMEX	MINWINL PLUS MINWINR EXCEEDS SESSLIM

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS or QUALIFY=DEFINE macroinstruction was issued and either the sum of MINWINL plus MINWINR is greater than the SESSLIM value specified, or the sum of DMINWNL plus DMINWNR is greater than the DSESLIM value specified.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0008'	USF6LNIN	SUPPLIED LENGTH INSUFFICIENT

The application issued one of the following macroinstructions:

- APPCCMD CONTROL=RCVEXPD
- APPCCMD CONTROL=RCVFMH5
- APPCCMD CONTROL=RECEIVE,OPTCD=XBUFLST
- APPCCMD CONTROL=OPRCNTL,QUALIFY=ACTSESS
- APPCCMD CONTROL=OPRCNTL,QUALIFY=DISPLAY
- APPCCMD CONTROL=OPRCNTL,QUALIFY=RESTORE
- APPCCMD CONTROL=TESTSTAT.

The data area or data length was not suitable as indicated in the following list:

RECEIVE,OPTCD=XBUFLST
The area specified is not large enough to hold one extended buffer list entry.

RCVEXPD
Data area is too small to contain all the expedited data.

RCVFMH5
Data area is too small to contain the next available FMH-5

QUALIFY=ACTSESS
Data length indicated in the supplied session parameters was larger than the amount of data provided or exceeds the maximum size allowed

QUALIFY=DISPLAY
Data area is too small to contain the DEFINE/DISPLAY (ISTSLD) structure

QUALIFY=RESTORE
Data area is too small to contain the RESTORE (ISTREST) structure

TESTSTAT
Data area is too small to contain the status data structure (ISTSTATD).

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0009'	USF6INSL	INCOMPLETE STRUCTURE SUPPLIED

The application program issued one of the following macroinstructions:

- APPCCMD CONTROL=OPRCNTL, QUALIFY=ACTSESS
- APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS
- APPCCMD CONTROL=OPRCNTL, QUALIFY=DEFINE.

The data length was not suitable as indicated in the following list:

QUALIFY=ACTSESS
Data length provided was less than the minimum size for the session parameters

QUALIFY=CNOS
Data length provided was less than the minimum size for the session limits structure (ISTSLCNS)

QUALIFY=DEFINE
Data length provided was less than the minimum size for the DEFINE/DISPLAY (ISTSLD) structure

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'000A'	USF6INFM	INCOMPLETE FMH5 SUPPLIED

The application program issued APPCCMD CONTROL=ALLOC, but did not supply an entire FMH-5.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'000B'	USF6INGD	INCOMPLETE GDS VARIABLE SUPPLIED

The application program issued an abnormal termination APPCCMD deallocation macroinstruction, but did not supply an entire GDS variable.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'000C'	USF60EXT	ZERO EXIT FIELD

The RPL specified that the ECB-EXIT field is being used as an EXIT field, but the RPL exit routine address in the field is zero. No RPL exit routine has been scheduled.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'000D'	USF60ECB	ZERO ECB FIELD

The RPL specified that the ECB-EXIT field is being used to point to an external ECB, but the address in the field is zero. No ECB has been posted.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'000E'	USF6RIAS	REQUEST INVALID FOR ADDRESS SPACE

A macroinstruction was issued in other than the ACB address space.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'000F'	USF6CBIN	CONTROL BLOCK INVALID

The RPL's ACB field does not contain the address of a valid ACB or the ACB is closed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0010'	USF6INDL	INVALID DATA ADDRESS OR LENGTH

An APPCCMD was issued that specified a work area address that is beyond the addressable range of the application program.

If using a buffer list or extended buffer list to send data, check entries to ensure that the length field does not contain any negative values.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0011'	USF6PRVO	PREVIOUS MACROINSTRUCTION OUTSTANDING

An APPCCMD is issued that specifies a conversation resource while an outstanding macroinstruction that targets the same conversation and processes on the same conversation queue is pending completion, or an APPCCMD CONTROL=OPRCNTL is issued while an outstanding operator control APPCCMD that targets the same LU is pending completion. Wait until the first macroinstruction completes or coordinate this request with the one that is outstanding.

For additional information on conversation queues, see the z/OS Communications Server: SNA Programmer's LU 6.2 Guide.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0012'	USF6BLIV	BUFFER LIST LENGTH INVALID

The RECLEN field of the RPL was not valid.

For the following macroinstructions, the RECLEN field must be a nonzero multiple of 16:

- APPCCMD CONTROL=DEALLOC, OPTCD=BUFFLST
- APPCCMD CONTROL=PREPRCV, OPTCD=BUFFLST
- APPCCMD CONTROL=SEND, OPTCD=BUFFLST
- APPCCMD CONTROL=SENDEXPD, OPTCD=BUFFLST
- APPCCMD CONTROL=SENDRCV, OPTCD=BUFFLST.

For the following macroinstructions, the RECLEN field must be a nonzero multiple of 48:

- APPCCMD CONTROL=DEALLOC, OPTCD=XBUFLST
- APPCCMD CONTROL=PREPRCV, OPTCD=XBUFLST
- APPCCMD CONTROL=SEND, OPTCD=XBUFLST

For the APPCCMD CONTROL=SENDRCV, OPTCD=XBUFLST macroinstruction, the value for RECLEN minus 16 must be a nonzero multiple of 48.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0013'	USF6NOMD	NO CORRESPONDING MODE IN LM TABLE

The application program issued one of the following macroinstructions:

- APPCCMD CONTROL=OPRCNTL, QUALIFY=DISPLAY
- APPCCMD CONTROL=OPRCNTL, QUALIFY=RESTORE.

The application program also specified a mode name for which no corresponding entry exists in the LU-mode table.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0014'	USF6IVBP	INVALID BIND PARAMETERS

The application program issued an APPCCMD CONTROL=OPRCNTL, QUALIFY=ACTSESS and specified a set of BIND parameters that were not valid, or the parameters in the BIND that was received were not valid.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0015'	USF6IVTP	INVALID TPN

The application program issued an APPCCMD CONTROL=ALLOC with an FMH-5 that contained a transaction program name that was reserved or not valid, such as X'06F1', which is the SNA service transaction program for the control operator.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0016'	USF6NOLU	NO CORRESPONDING LU IN LM TABLE

The application program issued one of the following macroinstructions:

- APPCCMD CONTROL=OPRCNTL, QUALIFY=DISPLAY
- APPCCMD CONTROL=OPRCNTL, QUALIFY=RESTORE.

The application program also specified an LU name for which no corresponding entry exists in the LU-mode table.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0017'	USF6IMDF	INVALID MODE SPECIFIED

The application program issued an APPCCMD CONTROL=OPRCNTL, QUALIFY=DEFINE macroinstruction and specified mode name SNASVCMG.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0018'	USF6ILSP	INVALID LIMIT SPECIFIED

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued and one of the session limit fields was an incorrect value.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0019'	USF6SMAI	SNASVCMG MODE ALREADY INITIALIZED

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued in order to initialize the SNASVCMG mode. However, it is already initialized, and no action was taken.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'001A'	USF6ALLS	ALL MODES SPECIFIED ON SINGLE SESSION LU

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued against all the mode names of the LU specified. However, the partner LU is single-session capable. Therefore, an APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction must be issued against a specific mode name.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'001B'	USF6SMSS	SNASVCMG OR CPSVCMG MODE FOR SINGLE SESSION LU

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued for the SNASVCMG or CPSVCMG mode name. However, the partner LU is single-session capable, and the SNASVCMG or CPSVCMG is not allowed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'001C'	USF6SSMI	SINGLE SESSION, MODE ALREADY INITIALIZED

An APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction was issued for a partner LU that is single-session capable. However, another of the LU's mode names is already initialized to nonzero session limits, and only one mode name can have nonzero session limits at a time.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'001E'	USF6CIDI	CID INVALID

The RPL's ARG field does not contain a valid session identifier (CID). You might have inadvertently modified the field or failed to set it in the first place, or you might have used the CID of a session that no longer exists.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'001F'	USF6APNA	APPCCMD ISSUED FOR NON-APPC

The application issued an APPCCMD against a non-LU 6.2 session or resource. The APPCCMD is rejected.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0020'	USF6PRRO	PREVIOUS REJECT REQUEST OUTSTANDING

An APPCCMD CONTROL=REJECT request was issued. However, a previous APPCCMD CONTROL=REJECT request has already been issued for the same resource. The later APPCCMD CONTROL=REJECT was rejected.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0021'	USF6DARJ	ABNORMAL DEALLOCATE REJECTED, RETRY

One of the following macroinstructions was issued:

- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDPROG
- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDSERV
- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDTIME
- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDUSER.

However, a prior macroinstruction that cannot be cancelled is outstanding. The command is not allowed in this case and is rejected. This command also is not allowed to be issued when the conversation is in RECEIVE state and no data has been received for the conversation. APPCCMD CONTROL=REJECT, QUALIFY=CONV can be issued to terminate the conversation and session in this case.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0022'	USF6IVCQ	INVALID CONTROL OR QUALIFY VALUE

An undefined value for the CONTROL or QUALIFY keyword was specified, or a QUALIFY value is not valid to use with the specified CONTROL value. For CONTROL types that do not use a QUALIFY value, RPL6QUAL must be set to zero.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0023'	USF6INSI	INVALID SESSION INSTANCE IDENTIFIER

VTAM rejected an APPCCMD CONTROL=REJECT, QUALIFY=SESSION request or an APPCCMD CONTROL=SETSESS, QUALIFY=SUSPEND request or an APPCCMD CONTROL=SETSESS, QUALIFY=RESUME request because the local application specified:

- A session instance identifier for a session that was not active at the time of the request
- A session ID length that was not valid.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0024'	USF6PSHI	PS HEADER NOT SUPPLIED

VTAM rejected the APPCCMD CONTROL=SEND request because the local application did not supply a complete PS header. (For example, the PS header length and data that follows are missing.)

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0025'	USF6PSLI	PS HEADER LENGTH IS INSUFFICIENT

VTAM rejected the APPCCMD CONTROL=SEND request because the local application specified an insufficient PS header length (the length equals 0).

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0026'	USF6NMSC	SESSION INSTANCE IDENTIFIER AND CONVERSATION IDENTIFIER MISMATCH

VTAM rejected the APPCCMD CONTROL=SETSESS, QUALIFY=SUSPEND request because the application program requested a session with APPCCMD CONTROL=SETSESS, QUALIFY=SUSPEND, but the conversation identified by CONVID was not currently assigned to the session identified by SESSID. VTAM rejected the request and nothing was suspended.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0027'	USF6IDET	INVALID DEACTIVATION TYPE CODE

VTAM rejected the APPCCMD CONTROL=REJECT, QUALIFY=SESSION request because the local application program omitted the DEACTYP parameter or specified an UNBIND deactivation type code value other than cleanup (X'0F') or protocol violation (X'FE'). The session has been successfully deactivated with UNBIND (X'0F').

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0028'	USF6NCRY	CRYPTOGRAPHY NOT ALLOWED ON MODE

An APPCCMD CONTROL=SEND, an APPCCMD CONTROL=PREPRCV, or an APPCCMD CONTROL=DEALLOC macroinstruction is rejected because CRYPT=YES is specified, and the mode does not support encryption.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0029'	USF6INLI	INVALID LIST VALUE SPECIFIED ON APPCCMD FOR RESTORE

The value for the LIST field in the RPL is not equal to NONE, ALL, or NOSESS. The keyword LIST=ALL, LIST=NONE, or LIST=NOSESS can be specified on the APPCCMD CONTROL=OPRCNTL, QUALIFY=RESTORE macroinstruction.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'002A'	USF6INCG	INVALID CGID VALUE SPECIFIED

A macroinstruction was issued specifying CONVGRP, but the conversation group ID (CGID) was not valid. You might have unintentionally modified the field, failed to set it correctly, or used a CGID that corresponds to a session that no longer exists.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'002B'	USF6NONI	NETWORK-QUALIFIED NAME REQUIRED

NETID was not coded on the APPCCMD although PARMS=(NQNAMES=YES) was coded on the ACB macroinstruction.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'002C'	USF6INEL	PARAMETER ERROR - INVALID EXPEDITED DATA LENGTH

An APPCCMD CONTROL=SENDEXPD was issued that specified an expedited data length of zero or an expedited data length greater than the allowed maximum. The largest expedited data size that can be sent with one macroinstruction invocation is 86 bytes.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'002D'	USF6INSC	PARAMETER ERROR - INVALID SENSE CODE VALUE SPECIFIED

An APPCCMD CONTROL=DEALLOC|DEALLOCQ,QUALIFY=ABNDUSER was specified with a sense code that was not an allocation or abnormal deallocation sense code value.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'002E'	USF6VANV	VECTOR AREA NOT VALID

The application supplied VTAM with a vector area address that is not valid or is write-protected.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'002F'	USF6VALI	VECTOR AREA LENGTH INSUFFICIENT

The application supplied VTAM with a vector area which is smaller than the minimum required size.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0030'	USF6STNV	PARAMETER_ERROR— STORAGE_TYPE_NOT_VALID

A storage type indication was not supplied or is invalid. Storage type is required to be specified via the ISTAPC82 mapping DSECT which is mapped within the ISTAPCVL mapping DSECT.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0031'	USF6VALS	PARAMETER_ERROR— SENDRCV_SPECIFIED _WITHOUT_ OPTCD=BUFFLST|XBUFLST

The APPCCMD CONTROL=SENDRCV was issued without specifying a buffer. OPTCD=BUFFLST|XBUFLST is required for this macroinstruction.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0032'	USF6UNXV	PARAMETER_ERROR— UNEXPECTED_VECTOR_ PROVIDED_ON_APPCCMD

An unexpected vector was provided on an APPCCMD request. An input vector is not defined for the APPCCMD.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0033'	USF6VNPV	PARAMETER_ERROR— A_REQUIRED_VECTOR_WAS_ NOT_PROVIDED_ OR_SPECIFIED_INCORRECTLY

A required input vector was either not provided or specified incorrectly on an APPCCMD request.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'002C'	X'0034'	USF6LNSP	PASSWORD_SUBSTITUTION_ VALUE_SET_IN_ERROR

The FMH-5 received from the application indicated password substitution in byte 4, bit 3. The session established with the partner does not support password substitution. Reissue the macroinstruction with this bit setting off.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0030'	X'0000'	USF6PENT	PROGRAM ERROR NO TRUNCATION

The remote transaction program issued an LU 6.2 SEND_ERROR verb specifying the TYPE(PROG) parameter; the conversation for the remote program was in a sending state; and the LU 6.2 SEND_ERROR verb did not truncate a logical record. No truncation occurs when a transaction program issues the LU 6.2 SEND_ERROR verb before sending any logical records or after sending a complete logical record. This return code is reported to the local application program when it issues an APPCCMD CONTROL=RECEIVE

macroinstruction prior to receiving any logical records or after receiving one or more complete logical records.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0034'	X'0000'	USF6PEPU	PROGRAM ERROR PURGING

The remote transaction program issued an LU 6.2 SEND_ERROR verb, specifying the TYPE(PROG) parameter, and the conversation for the remote transaction program was in RECEIVE state. The LU 6.2 SEND_ERROR verb might have caused information to be purged. Purging occurs when a transaction program issues the LU 6.2 SEND_ERROR verb in RECEIVE state before receiving all the information sent by the local application, that is, all the information sent prior to the reporting of the PROGRAM_ERROR_PURGING return code to the local application. The purging can occur at the local LU, the remote LU, or both. No purging occurs when a transaction program issues the LU 6.2 SEND_ERROR verb in a CONFIRM state, or in RECEIVE state after receiving all the information sent by the local application. This RCPRI code is normally reported to the local application on an APPCCMD it issues after sending some information to the remote transaction program. However, the RCPRI code can be reported on an APPCCMD the application issues prior to sending any information, depending on the CONTROL and QUALIFY fields of the APPCCMD and when it is issued. The conversation is in RECEIVE state.

Note: This code is never reported on an APPCCMD issued on a full-duplex conversation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0038'	X'0000'	USF6PETR	PROGRAM ERROR TRUNCATING

The remote transaction program issued an LU 6.2 SEND_ERROR verb, specifying the TYPE(PROG) parameter; the conversation for the remote transaction program was in a sending state; and the LU 6.2 SEND_ERROR verb truncated a logical record. Truncation occurs when a transaction program begins sending a logical record and then issues the LU 6.2 SEND_ERROR verb before sending the complete logical record. This return code is reported to the local application on an APPCCMD CONTROL=RECEIVE macroinstruction issued after receiving the truncated logical record. The conversation state is unchanged.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'003C'	X'0000'	USF6SENT	SERVICE ERROR NO TRUNCATION

The remote transaction program issued an LU 6.2 SEND_ERROR verb, specifying the TYPE(SVC) parameter; the conversation for the remote transaction program was in a sending state; and the LU 6.2 SEND_ERROR verb did not truncate a logical record. No truncation occurs when a transaction program issues the LU 6.2 SEND_ERROR verb before sending any logical records or after sending a complete logical record. This return code is reported to the local application on an APPCCMD CONTROL=RECEIVE macroinstruction it issues prior to receiving any logical records or after receiving one or more complete logical records. The conversation state is unchanged.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0040'	X'0000'	USF6SEPU	SERVICE ERROR PURGING

The remote transaction program issued an LU 6.2 SEND_ERROR verb, specifying the TYPE(SVC) parameter, and the conversation for the remote transaction program was in RECEIVE state. The LU 6.2 SEND_ERROR verb might have caused information to be purged. Purging occurs when a transaction program issues the LU 6.2 SEND_ERROR verb in RECEIVE state before receiving all the information sent by the local application, that is, all the information sent prior to the reporting of the SERVICE_ERROR_PURGING return code to the local application. The purging can occur at the local LU, the remote LU, or both. No purging occurs when a transaction program issues the LU 6.2 SEND_ERROR

verb in a CONFIRM state, or in RECEIVE state after receiving all the information sent by the local application. This return code is normally reported to the local application on an APPCCMD it issues after sending some information to the remote transaction program. However, the return code can be reported on an APPCCMD the application issues prior to sending any information, depending on the CONTROL and QUALIFY fields of the APPCCMD and when it is issued. The conversation is in RECEIVE state.

Note: This code is never reported on an APPCCMD issued on a full-duplex conversation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0044'	X'0000'	USF6SETR	SERVICE ERROR TRUNCATING

The remote transaction program issued an LU 6.2 SEND_ERROR verb, specifying the TYPE(SVC) parameter; the conversation for the remote transaction program was in a sending state; and the LU 6.2 SEND_ERROR verb truncated a logical record. Truncation occurs when a program begins sending a logical record and then issues the LU 6.2 SEND_ERROR verb before sending the complete logical record. This return code is reported to the local application on an APPCCMD CONTROL=RECEIVE macroinstruction issued after receiving the truncated logical record. The conversation state is unchanged.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0048'	X'0000'	USF6RFNR	RESOURCE FAILURE, NO RETRY

A failure occurred that caused the conversation to be prematurely terminated. For example, the session being used for the conversation was deactivated because of a session protocol error. The condition is not temporary, and the application should not try the transaction again until the condition is corrected. The conversation is in END_CONV or FDX_RESET state if no log data is present. If log data is present, the conversation is in PEND_END_CONV_LOG or PEND_RESET_LOG state.

Two common failures are:

1. Local LU sends unexpected control information.

   For example, the conversation can be in PENDING_DEALLOCATE state, but something other than a deallocate is received, or an FMH-7 is not received when it is expected.
2. Local LU sends unexpected data on the conversation.

   For example, a logical record that is not valid, PS header or FMH-7, might have been received, or a logical record is truncated by something other than an FMH-7.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'004C'	X'0000'	USF6RFRE	RESOURCE FAILURE, RETRY

A failure occurred that caused the conversation to be prematurely terminated. For example, the session being used for the conversation was deactivated because of a session outage, such as a line failure or a modem failure. The application can try the transaction again when the error that caused the session outage has been corrected. The conversation is in END_CONV or FDX_RESET state.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0050'	X'0000'	USF6STER	STATE ERROR

The specified conversation was not in an appropriate state to issue the specified APPCCMD. For example, the application program issued APPCCMD CONTROL=SEND, QUALIFY=DATA, but the conversation was in RECEIVE state. The state of the conversation remains unchanged.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0054'	X'0000'	USF6URMD	UNRECOGNIZED MODE NAME

The APPCCMD CONTROL=OPRCNTL, QUALIFY=CNOS macroinstruction did not execute successfully because the partner LU does not recognize the specified mode name. The local and partner LUs' CNOS parameters are not changed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0058'	X'0000'	USF6UNSC	UNSUCCESSFUL, SESSION NOT AVAILABLE

The APPCCMD CONTROL=ALLOC, QUALIFY=IMMED macroinstruction issued by the local application program did not execute successfully because there was not a contention-winner session available for use by a new conversation request. This RCPRI code is returned on the unsuccessful APPCCMD.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'005C'	(all)	USF6UECR	USER ERROR CODE RECEIVED

An FMH-7 was received that contained a sense code not interpreted by VTAM. The unrecognized sense code is passed to the application program through the SENSE field in the RPL extension. The application program must determine whether the sense code is a valid user-supplied sense code or a code that is not valid. The USER_ERROR_CODE_RECEIVED RCPRI code together with the following RCSEC subcodes (X'0000' X'0001') form the complete return code that is returned to the application. The subcode specifies whether a negative response preceded the FMH-7 containing the unrecognized sense code. The conversation is in a receiving state.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'005C'	X'0000'	USF6FNGR	FOLLOWING NEGATIVE RESPONSE

The FMH-7 containing the unrecognized sense code was received by VTAM following the receipt of a negative response.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'005C'	X'0001'	USF6WNGR	WITHOUT NEGATIVE RESPONSE

The FMH-7 containing the unrecognized sense code was not preceded by a negative response.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0060'	X'0000'	USF6NOFM	NO FMH5 AVAILABLE

The application issued an APPCCMD CONTROL=RCVFMH5, but there is currently no FMH-5 waiting to be received by the application program.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0064'	X'0000'	USF6ACFL	ACTIVATION FAILURE

An APPCCMD CONTROL=OPRCNTL, QUALIFY=ACTSESS macroinstruction did not execute successfully because activation for the pending active session failed. For example, the path between the application and the other LU could have been lost.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0068'	X'0000'	USF6SLEX	LU MODE SESSION LIMIT EXCEEDED

An APPCCMD CONTROL=OPRCNTL, QUALIFY=ACTSESS macroinstruction did not execute successfully because activating the pending active session would have caused the session limits for the mode name group to be exceeded.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'006C'	X'0000'	USF6SACT	SESSION NOT PENDING

An APPCCMD CONTROL=OPRCNTL, QUALIFY=ACTSESS or QUALIFY=DACTSESS macroinstruction was issued for a session that is no longer pending. The CID for the session is valid but a BIND or CINIT is no longer queued, or the session is being deactivated due to a previous error or request.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0070'	X'0000'	USF6STOR	TEMPORARY STORAGE SHORTAGE OR RESOURCE SHORTAGE

VTAM is unable to process the request because of a temporary storage shortage, a resource shortage, or other shortage.

- If a sense code is not provided, a temporary storage shortage has occurred.
- If a sense code is provided indicating insufficient resources, then a storage shortage or other resource shortage has occurred. In either of these cases, the request can be reissued (with EXECRPL, for example.) There is no state change. This return code is reported to the application program to allow time for the problem to diminish or disappear. If VTAM attempts to try the request again, the additional storage might not be available immediately, and the problem might occur again.
- If a sense code is provided other than one for insufficient resources, examine the sense code explanation to determine the action required. In this situation, whether the request can be reissued depends on the information contained in the sense code.
- If this return code is received at the completion of an APPCCMD with CONTROL=RECEIVE, OPTCD=(,XBUFLST), then a CSM buffer that meets the storage type specified in the XBUFLST-receive vector could not be obtained to receive the data, or other VTAM internal resources required to receive the data could not be obtained. The system is storage constrained. No data is received.

  The application can take several possible actions:

  – Reissue the APPCCMD several times as a temporary retry recovery action.
  – Issue a receive without the XBUFLST specification so the data can be copied into application private storage.
  – Explicitly deallocate the conversation via APPCCMD services.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0074'	X'0000'	USF6HALT	HALT ISSUED

The operator has issued a HALT command. Depending on the type of HALT, the application program can no longer issue certain macroinstructions. See the z/OS Communications Server: SNA Programmer's LU 6.2 Guide for more information on the effect of HALT upon the application.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0078'	X'0000'	USF6VIYA	VTAM INACTIVE FOR YOUR ACB

The association between VTAM and the application program (ACB) that was established with the OPEN macroinstruction has been broken (the ACB is in the process of being closed). This might have occurred because:

- The application program has elsewhere issued a CLOSE that has not yet completed
- VTAM has become inactive
- A VARY NET,INACT command was issued for the application program.

Any active conversations are placed in END_CONV or FDX_RESET state.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'007C'	X'0000'	USF6RQAB	REQUEST ABORTED

VTAM has rejected a request because of an error detected while processing the request or because of an error in the associated session, task, or address space. For example, an abend. If an abend code is available, see Chapter 7, “VTAM abend codes,” on page 307 to interpret the code. An abend might or might not be tried again.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0080'	X'0000'	USF6DLNR	DEALLOCATE NORMAL

The remote transaction program issued an LU 6.2 DEALLOCATE TYPE(FLUSH) verb. This return code is reported to the application program on an APPCCMD CONTROL=SEND, QUALIFY=ERROR macroinstruction issued when the conversation is in RECEIVE state. The conversation is in END_CONV state. The conversation can be in RECEIVE state or in PEND_RCV_LOG state. This return code applies only to half-duplex conversations.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0084'	X'0000'	USF6STSH	STORAGE SHORTAGE

Indicates VTAM has encountered a storage shortage when attempting to satisfy an APPCCMD CONTROL=RECEIVE or an APPCCMD CONTROL=RCVFMH5, either while storing incoming data or sending a pacing response. There is no state change.

This return code can also be issued when a storage failure occurs while processing an internal DEALLOC FLUSH request. VTAM does internal DEALLOC FLUSH processing when it receives an indication that the partner has issued an abnormal deallocation request on the full-duplex conversation.

The application should issue one of the abnormal termination APPCCMD CONTROL=DEALLOC|DEALLOCQ macroinstructions to end the conversation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0088'	X'0000'	USF6CREJ	CANCELED BY REJECT OR ABNORMAL DEALLOCATE

The request, while in progress, was canceled by the issuance of an APPCCMD CONTROL=REJECT or abnormal deallocation APPCCMD, which has requested the termination of the current conversation and, possibly, the session.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'008C'	X'0000'	USF6PROE	PARTNER COMMITTED PROTOCOL VIOLATION

The partner LU has violated conversation protocols during the execution of this command. Notification of conversation failure will be received on a subsequent APPCCMD command. There is no state change.

Two common protocol violations are:

- Partner LU sends unexpected control information.

  For example, the conversation can be in PENDING_DEALLOCATE state, but something other than a deallocate is received, or an FMH-7 is not received when it is expected.
- Partner LU sends unexpected data on the conversation.

  For example, a logical record that is not valid, PS header or FMH-7, might have been received, or a logical record is truncated by something other than an FMH-7.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0090'	X'0000'	USF6NOTA	APPLICATION NOT APPC CAPABLE

The application program issued an APPCCMD, but the application program has APPC=NO coded on its APPL definition statement. The APPL definition statement must have APPC=YES coded before the application program can issue APPCCMD macroinstructions.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0094'	X'0000'	USF6SDRJ	INVALID CONDITION FOR SENDING DATA

This indicates that the application program issued an APPCCMD that provided data to be sent following an error on a previous QUALIFY=DATAFLU or QUALIFY=DATACON type of send (either CONTROL=SEND, CONTROL=PREPRCV or CONTROL=DEALLOC). However, data remains, held by VTAM, from the error on the previous DATAFLU or DATACON macroinstruction.

Before sending more data, issue a macroinstruction that flushes VTAM's buffers. An APPCCMD CONTROL=SEND, QUALIFY=FLUSH macroinstruction, an APPCCMD CONTROL=SEND, QUALIFY=ERROR macroinstruction, or one of the abnormal termination CONTROL=DEALLOC macroinstructions will flush the send data queue so that processing can continue.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'0098'	X'0000'	USF6STGS	TEMPORARY STORAGE SHORTAGE WHILE SENDING DATA

This indicates a temporary storage shortage has occurred while sending data. This RCPRI, RCSEC combination might be returned for one of the following macroinstructions:

- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDPROG
- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDSERV
- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDTIME

- APPCCMD CONTROL=DEALLOC, QUALIFY=ABNDUSER
- APPCCMD CONTROL=DEALLOCQ, QUALIFY=ABNDPROG
- APPCCMD CONTROL=DEALLOCQ, QUALIFY=ABNDSERV
- APPCCMD CONTROL=DEALLOCQ, QUALIFY=ABNDTIME
- APPCCMD CONTROL=DEALLOCQ, QUALIFY=ABNDUSER
- APPCCMD CONTROL=DEALLOC, QUALIFY=DATACON
- APPCCMD CONTROL=DEALLOC, QUALIFY=DATAFLU
- APPCCMD CONTROL=PREPRCV, QUALIFY=DATACON
- APPCCMD CONTROL=PREPRCV, QUALIFY=DATAFLU
- APPCCMD CONTROL=SEND, QUALIFY=DATA
- APPCCMD CONTROL=SEND, QUALIFY=DATACON
- APPCCMD CONTROL=SEND, QUALIFY=DATAFLU
- APPCCMD CONTROL=SEND, QUALIFY=ERROR
- APPCCMD CONTROL=SENDRCV, QUALIFY=DATAFLU

The current position in the application-supplied data buffer (the area pointed to by the AREA field of the RPL) is returned in RPL6STBF (the current buffer) and RPL6STDS (displacement in the data). All data prior to this buffer or buffer list entry has been sent.

The user has two alternatives when this return code is received.

- Attempt to continue sending data on the conversation by issuing an APPCCMD macroinstruction with the data pointers and length set to reflect the values returned in RPL6STBF and RPL6STDS. The subsequent macroinstruction must be issued with the AREA field set with the RPL6STBF value plus the RPL6STDS value to avoid duplicating any data already sent. The data length (the RECLEN field in the RPL) must also be adjusted to indicate the amount of remaining data. Once the subsequent macroinstruction with the updated data location completes successfully, the conversation can be continued as if the storage shortage did not occur.

  For more information on how to process the remaining data, see the z/OS Communications Server: SNA Programmer's LU 6.2 Guide.
- Deactivate the conversation by issuing one of the abnormal termination CONTROL=DEALLOC macroinstructions, or APPCCMD CONTROL=REJECT macroinstructions. Note that REJECT must be issued to deactivate a conversation if the abnormal termination CONTROL=DEALLOC macroinstructions are unsuccessful.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'009C'	X'0001'	USF6RSTF	RESTORE REJECTED—RESTORE ISSUED BEFORE SETLOGON START

The APPCCMD CONTROL=OPRCNTL, QUALIFY=RESTORE macroinstruction is issued before the SETLOGON START macroinstruction is issued.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	(all)	USF6RNAL	REQUEST NOT ALLOWED

VTAM rejected the APPCCMD because the macroinstruction request conflicts in some way with the capabilities of the session or conversation to which it applies. The REQUEST_NOT_ALLOWED RCPRI code together with one of the following RCSEC subcodes form the complete return code that is returned to the transaction program.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	X'0001'	USF6LNSE	LU PAIR DOES NOT SUPPORT SENDING EXPEDITED DATA

VTAM rejected the APPCCMD CONTROL=SENDEXPD because the negotiated support level of the current session does not support protocols needed to transmit expedited data.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	X'0002'	USF6RQBL	REQUEST BLOCKED

VTAM rejected the APPCCMD because the conversation with which it is associated is in the process of being deallocated or terminated.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	X'0003'	USF6RNEX	EXECUTION OF REQUEST TERMINATED

VTAM rejected an APPCCMD CONTROL=RCVEXPD, QUALIFY=SPEC on a half-duplex conversation because the partner LU is awaiting a change-direction or end-of-chain indicator before sending error information. No expedited information was available to be received.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	X'0004'	USF6VNVF	CONTROL/QUALIFY VALUE INVALID FOR FULL-DUPLEX CONVERSATION

VTAM rejected the APPCCMD because the CONTROL= and QUALIFY= value combination specified is not allowed for a full-duplex conversation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	X'0005'	USF6EXRO	RSP HAS NOT BEEN RECEIVED FOR A PREVIOUS SENDEXPD REQUEST

VTAM rejected a APPCCMD CONTROL=SENDEXPD,QUALIFY=DATA or an APPCCMD CONTROL=SEND, QUALIFY=RQSEND because the response to a previously issued APPCCMD CONTROL=SENDEXPD,QUALIFY=DATA had not been received from the partner LU.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	X'0006'	USF6NAUT	PROGRAM_NOT_AUTHORIZED_ FOR_REQUESTED_FUNCTION

An application not using VTAM authorized path attempted to use the HPDT interface. The request is disallowed.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A0'	X'0008'	USF6ENEL	NAMED RESOURCE NOT ELIGIBLE FOR REQUESTED ALTERATION

A MODIFY DEFINE command with DELETE=UNUSE was issued for an entry in the LU-mode table, but the entry type is not UNUSABLE.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A4'	X'0000'	USF6SPMD	MODE MUST BE RESTORED BEFORE USING

An APPCCMD macroinstruction is issued with a mode name that is pending recovery for persistent LU-LU sessions. Issue the APPCCMD CONTROL=OPRCNTL, QUALIFY=RESTORE macroinstruction to restore the mode.

Note: For more information on which macroinstructions can be issued for modes that are pending recovery for persistent LU-LU sessions, see the z/OS Communications Server: SNA Programmer's LU 6.2 Guide.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A8'	(all)	USF6ENVE	ENVIRONMENT ERROR

A macroinstruction has failed for some reason related to the system environment in which the request was processed. The RCSEC subcode identifies the specific error.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A8'	X'0000'	USF6OSLV	OS LEVEL DOES NOT SUPPORT REQUESTED FUNCTION

A macroinstruction request required the use of an operating system service which is not supported by the active operating system level.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A8'	X'0001'	USF6XMES	SUSPEND FAILURE

VTAM attempted to suspend processing of an APPCCMD macroinstruction issued in either cross-memory mode or in synchronous SRB-mode with OPTCD=KEEPSRB specified. The attempt failed, probably due to conditions in the operation system environment. The application may reissue the request.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00A8'	X'0002'	USF6XMER	RESUME FAILURE

VTAM attempted to resume processing of an APPCCMD macroinstruction issued in either cross-memory mode or in synchronous SRB-mode with OPTCD=KEEPSRB specified. The attempt failed. VTAM is unable to post the request complete. If the application has a LOSTERM exit, it will be scheduled with a reason code of 44. For more information about the LOSTERM exit, see the z/OS Communications Server: SNA Programming . The RPL is now available for reuse.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	(all)	USF6ERIN	ERROR INDICATION RECEIVED

VTAM's processing of an APPCCMD request stored on the SEND queue of a full-duplex conversation was ended because the remote transaction program or LU issued an LU 6.2 architecture verb that cancelled

further processing of the request. An associated Secondary Return Code value indicates the type of operation that caused the request to be ended.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	X'0001'	USF6EIAS	DEALLOCATE ABEND PROGRAM

An APPCCMD that processes on the SEND queue of a full-duplex conversation was terminated because an abnormal deallocation request was issued by the remote transaction program. The FMH-7 received from the partner LU carried a sense code indicating that the remote transaction program issued a DEALLOCATE verb with TYPE(ABEND_PROG).

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	X'0002'	USF6ERAS	DEALLOCATE ABEND SERVICE

An APPCCMD that processes on the SEND queue of a full-duplex conversation was terminated because an abnormal deallocation request was issued by the remote transaction program. The FMH-7 received from the partner LU carried a sense code indicating that the remote transaction program issued a DEALLOCATE verb with TYPE(ABEND_SVC).

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	X'0003'	USF6EIAT	DEALLOCATE ABEND TIME

An APPCCMD that processes on the SEND queue of a full-duplex conversation was terminated because an abnormal deallocation request was issued by the remote transaction program. The FMH-7 received from the partner LU carried a sense code indicating that the remote transaction program issued a DEALLOCATE verb with TYPE(ABEND_TIMER).

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	X'0004'	USF6EIAT	ALLOCATION ERROR

An APPCCMD that processes on the SEND queue of a full-duplex conversation was terminated because an abnormal deallocation request was issued by the remote transaction program. The FMH-7 received from the partner LU carried a sense code indicating that an Allocation request was rejected by the remote transaction program.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	X'0005'	USF6EIUN	UNKNOWN ERROR CODE

An APPCCMD that processes on the SEND queue of a full-duplex conversation was terminated because an abnormal deallocation request was issued by the remote transaction program. The FMH-7 received from the partner LU carried a sense code other than the Deallocate ABEND, Allocation Error, or Resource Failure codes. The application program must determine whether the sense code is a valid user-supplied sense code or is an invalid code.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	X'0006'	USF6EIRR	RESOURCE FAILURE, RETRY

An APPCCMD that processes on the SEND queue of a full-duplex conversation was terminated because a failure occurred that caused the conversation to be prematurely terminated. The application can try the transaction again when the error that caused the session outage has been corrected.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00AC'	X'0007'	USF6EIRN	RESOURCE FAILURE, NO RETRY

An APPCCMD that processes on the SEND queue of a full-duplex conversation was terminated because a failure occurred that caused the conversation to be prematurely terminated. The condition is not temporary, and the application should not try the transaction again until the condition is corrected.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'(all)'	USF6NRER	NAME RESOLUTION ERROR

VTAM rejected an APPCCMD because there was an inappropriate name translation. The NAME_RESOLUTION_ERROR RCPRI code together with one of the following RCSEC subcodes form the complete return code that is returned to the transaction program.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0001'	USF6NRRE	LUNAME FOUND IN A VARIANT NAME ENTRY

VTAM rejected an APPCCMD because the LUNAME specified on the macroinstruction was found in a VARIANT_NAME entry in the LU-mode table.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0002'	USF6NRRD	NAME RETURNED DIFFERS FROM ASSOCIATED NAME

VTAM rejected an APPCCMD because the BIND RSP contained an LUNAME that is different from the associated name in the SUPPLIED_NAME entry in the LU-mode table. The association of names for the partner LU had previously occurred.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0003'	USF6NRRA	NAME RETURNED FOUND IN VARIANT_NAME ENTRY

VTAM rejected an APPCCMD because the LUNAME returned in the BIND RSP was found in a VARIANT_NAME entry in the LU-mode table. The association of names for the partner LU has not occurred.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0004'	USF6NRAP	NAME RETURNED FOUND IN SUPPLIED_NAME ENTRY

VTAM rejected an APPCCMD because the LUNAME contained in the BIND RSP was found in a SUPPLIED_NAME entry in the LU-mode table. The SUPPLIED_NAME entry was different than the entry used in the session initiation.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0005'	USF6NRNM	PARTNER NETWORK NAME MISMATCH

VTAM rejected an APPCCMD because the NETID contained in the BIND RSP was different than that previously saved in the LU-mode table for that LUNAME.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0006'	USF6NRAV	LUNAME FOUND IN AN UNUSABLE_NAME ENTRY

VTAM rejected an APPCCMD because the LUNAME specified on the macroinstruction was found in an UNUSABLE_NAME entry in the LU-mode table.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0007'	USF6NRRE	NAME RETURNED FOUND IN AN UNUSABLE_NAME ENTRY

VTAM rejected an APPCCMD because the partner LU returned an LUNAME in the BIND response that was found in an UNUSABLE_NAME entry in the LU-mode table.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B0'	X'0008'	USF6NRDN	LU NAME FOUND IN A DISASSOCIATED_NAME ENTRY

VTAM rejected an APPCCMD macroinstruction request or an operator command because the LU name specified is a DISASSOCIATED_NAME entry. This type of entry has no mode values and thus has no sessions. The LU name was previously a VARIANT_NAME entry but is no longer associated with a SUPPLIED_NAME entry.

If the request or operator command was to display information about the LU, reissue the request with a with LOGMODE=0 and any LU-specific information will be returned.

If the request was for an allocate, a CNOS must be issued to establish mode information before the allocate can be tried again.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B4'	(all)	USF6CSME	CSM_DETECTED_ERROR

CSM detected an error. The CSM_DETECTED_ERROR RCPRI code together with one of the following RCSEC subcodes form the complete return code that is returned to the transaction program.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B4'	X'0001'	USF6NSPC	CSM_DETECTED_ERROR–NOT_SPECIFIED

CSM detected a problem during APPCCMD processing of the request. The specific reason for the error is not passed back to the APPCCMD application.

Upon receipt of this return code the application can:

- Optionally consider the error temporary and try the request again several times.

  Note that it is possible that the error might not recur. This temporary error condition could occur in the case where a VTAM-built parameter list to CSM is randomly corrupted on a particular request, but not on a subsequent request.
- Consider the error permanent and terminate the conversation.

See the z/OS Communications Server: CSM Guide for more information about these CSM errors.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B4'	X'0002'	USF6IBTK	CSM_DETECTED_ERROR—INVALID_BUFFER_ TOKEN_SPECIFIED

The communications storage manager (CSM) detected a problem during APPCCMD processing of the request. The specific reason for the error is that CSM detected that the CSM buffer token being used for the APPCCMD is not a valid CSM buffer token.

Upon receipt of this return code the application can:

- Check the current buffer pointer (RPL6STBF) in the RPL extension to determine the address of the buffer list entry that was processed when the error occurred.
- Optionally consider the error temporary and try the request again several times.

  Note that it is possible that the error might not recur. This temporary error condition could occur in the case where a VTAM-built parameter list to CSM is randomly corrupted on a particular request, but not on a subsequent request.
- Consider the error permanent and terminate the conversation.
- Continue using the conversation with a different CSM buffer.

See the z/OS Communications Server: CSM Guide for more information about these CSM errors.

RCPRI	RCSEC	ISTUSFBC EQU label	Meaning
X'00B4'	X'0003'	USF6IIID	CSM_DETECTED_ERROR—INVALID_INSTANCE_ ID_SPECIFIED

The communications storage manager (CSM) detected a problem during APPCCMD processing of the request. The specific reason for the error is that CSM detected that the instance ID portion of the CSM buffer token being used for the APPCCMD is not a valid CSM instance ID. Because the instance ID is not valid, it is possible that the CSM buffer that is being specified on the APPCCMD was previously freed and a new instance ID was assigned to the storage by CSM.

Upon receipt of this return code the application can:

- Check the current buffer pointer (RPL6STBF) in the RPL extension to determine the address of the buffer list entry that was processed when the error occurred.
- Optionally consider the error temporary and try the request again several times.

  Note that it is possible that the error might not recur. This temporary error condition could occur in the case where a VTAM-built parameter list to CSM is randomly corrupted on a particular request, but not on a subsequent request.
- Consider the error permanent and terminate the conversation.
- Continue using the conversation with a different CSM buffer.

See the z/OS Communications Server: CSM Guide for more information about these CSM errors.

LAN channel station error return codes

The LAN channel station error return codes provide a consistent platform to report the status of user requests or abnormal conditions detected by the service provider. The error return codes are used on the following occasions.

- If an error or exceptional condition is detected during the execution of a request, the error code is carried as the completion codes in the corresponding response.
- If an error or exception condition is asynchronously detected by the service provider while no related request from the service user is outstanding, the error code is reported as a part of the common status in a provider-initiated request, such as Close_Station_Indication.

The following list contains frequently used abbreviations.

802.2
IEEE LAN Standard 802.2

802.3
IEEE LAN Standard 802.3

802.4
IEEE LAN Standard 802.4

802.5
IEEE LAN Standard 802.5

IEEE
Institute of Electrical and Electronic Engineers

LAN
Local area network

LLC
Logical link control

MAC
Medium access control

SAP
Service access point

The two-byte LAN return codes are based on the architectural layer that detected the error. Byte 0 is the general classification, and Byte 1 is the specific completion code.

Byte 0—LAN general classifications

- X'20' MAC generic

  This value is used for all MAC-level protocols, including high-level link control (HDLC) as well as LANs.
- X'22' MAC LAN specific

  This value is used for LAN MAC-level protocols.
- X'70' LLC generic

  This value is used for all LLC-level protocols.
- X'76' LLC LAN specific

  This value is used for LLC MAC-level protocols.

The following tables contain all the completion codes currently supported by link service architecture (LSA) for the LAN environment.

MAC generic codes

Table 5. MAC generic codes

Code	Meaning	Explanation
2000	Done	The MAC command was successfully completed.
2001	Identifier not valid	The MAC detected that the data in the identifier field was blank, syntactically incorrect, or otherwise unrecognizable.
2002	State error	The MAC received a primitive that was illogical for the current MAC state.
2003	ID type not valid	The MAC detected that the data in the ID type field was blank, syntactically incorrect, or otherwise unrecognizable.
2004	Primitive code not valid	The MAC received a request with a primitive code that was not valid or a primitive code for an unsupported request.
2005	Control information length not valid	The MAC received a primitive in which the control information length was incorrect for the primitive type.
2006	Length-of-data area not valid	The MAC received a request that specified a length-of-data area that was not valid.
2007	Interface data not valid	The MAC detected that the data in the interface data field was missing, blank, syntactically incorrect, or otherwise unrecognizable.
2008	No resource	During initialization the MAC layer was unable to obtain a required resource. Processing cannot continue until the resource is available.
2009	MAC receive error	An error occurred while receiving a frame.
200A	Transmit error	An error occurred during the transmission of the information in a MAC_DATA request. As a result, the transmission was terminated.
200B	MAC unexpected interrupt	The MAC layer detected an unexpected (not valid) interrupt.
200C	Frame check sequence (FCS) threshold reached	The link threshold counter for the number of FCS errors reached its limit.
200D	Aborted by MAC_DEACTIVATE_SAP	The MAC issued a MAC_DEACTIVATE_SAP indication, requesting closing of the station.
200E	Path error	The MAC layer reported a path error, including hardware errors.
200F	Resource not available	A request for an unavailable resource was received.
2010	Layer already enabled	A request to enable a MAC layer was received for a layer that is already enabled. This code does not signify an error condition.
2011	Maximum MSDU size too large	MAC_ENABLE request received in which the size specified for the MAC service data unit is larger than the capabilities of the MAC layer.

Table 5. MAC generic codes (continued)		
Code	**Meaning**	**Explanation**
2012	MSDU size not valid	The size of the MAC service data unit in a MAC_DATA request is not valid.
2013	MAC instance not valid	The MAC instance name specified is not valid.
2014	MAC layer not enabled	A request was made of the MAC layer, but the layer is not enabled.
2015	Port ID not valid	The port identifier specified in the corresponding request is not valid. The request is rejected.
2016	Invalid MAC address	The MAC address specified in the request is invalid.
2017	SAP already activated	The SAP requested to be activated in the ACTIVATE_SAP request is already active. The request is rejected.
2018	Adapter disabled	The request is rejected because the MAC layer is not active.
2019	SAP ID not found SAP not activated	The provider SAP specified in the request could not be found or is not active.
201A	Service type not valid	Service type requested on the MAC_ACTIVATE_SAP request was not a type known to the MAC layer.
201B	Service already activated (user identified)	Service type requested in the MAC_ACTIVATE_SAP has already been specified by another user. The request is rejected.
201C	Service not previously activated	Service type to be deactivated in a MAC_DEACTIVATE_SAP request was not previously active.
201D	MAC disabled SAPs deactivated	MAC disabled and SAPs successfully deactivated.
201E	Layer enabled successfully	MAC_ENABLE request successfully completed.
201F	SAP deactivated	MAC_DEACTIVATE_SAP request successfully completed.

MAC LAN specific codes

Table 6. MAC LAN specific codes		
Code	**Meaning**	**Explanation**
2201	Ether_type (802.3) not valid	Type field specified for ethernet was not valid. This is a completion code common to all primitives when Ethernet or IEEE 802.3 service is requested.
2202	Force_IMPL_enable (802.5) not valid	This completion code is returned in response to a MAC_ENABLE request. A request to force a program load was not valid, possibly because the station has not allowed a remote program load.
2204	Initialize options (802.5) not valid	The parameters requested to initialize the token-ring MAC layer are not valid.

Table 6. MAC LAN specific codes (continued)

Code	Meaning	Explanation
2205	Open options (802.5) not valid	Some of the parameters on the MAC_ENABLE request are not valid. The request is rejected.
2206	Rx_burst_size (802.5) not valid	When data was being received or repeated, a sequence of four or more half-bit times were received without transition. This occurrence is not valid in the token-ring protocol.
2207	Group address not valid	The group address specified in the MAC_ACTIVATE_SAP request is not valid. See the *IBM Token-Ring Network Architecture Reference* for the format of a group address.
2208	Functional address (802.5) not valid	This completion code applies only to token ring. The functional address specified in the MAC_ACTIVATE_SAP request is not valid or has the wrong format. See the *IBM Token-Ring Network Architecture Reference* for the format of the defined functional addresses.
2209	Group/logical address conflict	The group address specified in the MAC_ACTIVATE_SAP request is in conflict with previously assigned MAC group addresses.
220A	Function class conflict (802.5)	The functional address specified in the MAC_ACTIVATE_SAP request is in conflict with previously assigned MAC functional addresses. See the *IBM Token-Ring Network Architecture Reference* for more information.
220B	Duplicate MAC address	The MAC address specified in the MAC_ENABLE request is already present in the ring. The request is rejected in order to prevent duplicate addresses.
220C	Attribute type not valid	This completion code is returned in response to a RTV_ATTRIB request. It indicates that the attribute type specified in the primitive is not valid.
220D	Frame priority not valid	This completion code is returned in response to a MAC_DATA request. It indicates that the requested priority of the frame is not valid.
220E	Function class vector length (802.5) not valid	This completion code is returned in response to a MAC_ACTIVATE_SAP request. It indicates that the length specified in the request for the function class vector is not valid.
220F	Function class (802.5) not valid	This completion code is returned in response to a MAC_ACTIVATE_SAP request. It indicates that a function class specified in the request was not valid. See the *IBM Token-Ring Network Architecture Reference* for the valid function classes.
2210	Destination address not valid	This completion code is returned in response to a MAC_DATA request. It indicates that the destination address specified in the request is not valid.

Table 6. MAC LAN specific codes (continued)

Code	Meaning	Explanation
2211	Frame type not valid	This completion code is returned in response to a MAC_DATA request. It indicates that the frame type specified in the request is not valid. See the *IBM Token-Ring Network Architecture Reference* for a definition of the valid frame types.
2212	Frame control not valid	This completion code is returned in response to a MAC_DATA request. It indicates that the frame control field specified in the request is not valid. See the *IBM Token-Ring Network Architecture Reference* for a definition of the valid frame control fields.
2213	Unauthorized access priority	This completion code is returned in response to a MAC_DATA request. It indicates that the ring access priority requested for the frame is not valid. See the *IBM Token-Ring Network Architecture Reference* for a description of the priorities.
2214	Unauthorized MAC frame	This completion code is returned in response to a MAC_DATA request. It indicates that the MAC frame requested to be transmitted is not authorized. See the *IBM Token-Ring Network Architecture Reference* for a list of the various MAC frames and the authorization needed to transmit them.
2215	Address not recognized	This completion code is returned in response to a MAC_DATA request. It indicates that the MAC address specified in the frame was not recognized by any station on the local ring. Specifically, the address-recognized (A) bits were not set in the frame status field in the returned frame. See the *IBM Token-Ring Network Architecture Reference* for the format of the frame status field and the use of the A bits.
2216	Frame not copied	This completion code is returned in response to a MAC_DATA request. It indicates that the MAC address specified in the frame was recognized by a station on the ring, but the station was unable to copy the frame. Specifically, the address-recognized (A) bit was set, but the frame-copied (C) bits were not set in the returned frame. See the *IBM Token-Ring Network Architecture Reference* for format of the frame status field and the use of the A and C bits.
2217	Ring status error (802.5)	An error occurred on the ring during the processing of the request.
2218	Adapter check error	An adapter check occurred when processing the corresponding request.
2219	Force IMPL enable (802.5) not valid	A program load was requested but was invalid.
221A	Open error (802.5)	This completion code is returned in response to a MAC_ENABLE request. It indicates that an error occurred when attempting to enable the MAC layer.

Table 6. MAC LAN specific codes (continued)		
Code	**Meaning**	**Explanation**
221B	Mode (802.3/4) not valid	This completion code is returned in response to a MAC_ENABLE request. It indicates that a copy was requested but was not valid.
221C	Net type (802.3) not valid	This completion code indicates that the net type specified in the request is not valid.
221D	In_ring_desired (802.4) not valid	This completion code is returned in response to a MAC_ENABLE request. It indicates that the value specified for the In_ring_desired parameter is not one of the defined values.
221E	Min_Post_Silence_ Preamble_Length (802.4) not valid	This completion code is returned in response to a MAC_ENABLE request. It indicates that the value specified for the minimum time the station must idle after silence is not valid.
221F	Maximum Number of SAPs exceeded	This completion code is returned in response to a MAC_ACTIVATE_SAP request. It indicates that the maximum number of SAPs have been activated. The request is rejected.
2220	Field length not valid	This completion code is returned in response to a MAC_DATA request. It indicates that the length of the routing information field is larger than this MAC can handle.
2221	MSDU length not valid	This completion code is returned in response to a MAC_DATA request. It indicates that the value specified as the length of the MAC service data unit is not valid.
2222	Retries exhausted	This completion code is returned in response to a request-with-response on a MAC_DATA request. It indicates that the protocol data unit (PDU) was transmitted such that the retries were exhausted, but no response was received. It is used in conjunction with LLC Type 3 service.

LLC LAN generic codes

Table 7. LLC LAN generic codes		
Code	**Meaning**	**Explanation**
7000	Done	The LLC command was successfully completed.
7001	ID not valid	The LLC detected that the data in the ID field was blank, syntactically incorrect, or otherwise unrecognizable.
7002	State error	The LLC received a primitive that was illogical for the current LLC state.
7003	ID type not valid	The LLC detected that the data in the ID type field was blank, syntactically incorrect, or otherwise unrecognizable.

Table 7. LLC LAN generic codes (continued)		
Code	**Meaning**	**Explanation**
7004	Primitive not valid	The LLC received a request with a primitive code that was not valid or a primitive code for an unsupported request.
7005	Control information length not valid	The LLC received a primitive in which the control information length was incorrect for the primitive type.
7006	Length-of-data area not valid	The LLC received a request that specified a length-of-data area that was not valid.
7007	Interface data not valid	The LLC detected that the data in the interface data field was missing, blank, syntactically incorrect, or otherwise unrecognizable.
7008	Primitive not recognized	The primitive code in the request received by LLC is not one of the recognized primitives. This return code indicates a LLC user error.
700B	Unsupported service type	An N_ACTIVATE_SAP or N_DEACTIVATE_SAP request was received, specifying an invalid service type.
700C	Service type not activated	An N_DEACTIVATE_SAP request was received, but the particular manager was not active. Either an N_ACTIVATE_SAP request was not issued or an N_DEACTIVATE_SAP request was issued prior to LLC receiving this request. This code usually indicates an LLC user error.
7010	Service type already activated	An N_ACTIVATE_SAP request was received, but the service was already active. This code usually indicates an LLC user error.
7012	Requestor not manager of service	An N_DEACTIVATE_SAP request was received on a CID (connection ID) other than that of the manager of the service. This code usually indicates an LLC user error.

LLC LAN specific codes

Table 8. LLC LAN specific codes		
Code	**Meaning**	**Explanation**
7603	Layer instance program check	The instance of the LLC receiving the primitive encountered a program check. As a result the LLC layer was unable to process the request. This completion code can be used in response to any of the LLC primitives.
7604	System error	The system in which the LLC is running encountered an error. As a result, the LLC layer was unable to process the request. This completion code can be used in response to any of the LLC primitives.
7605	MAC instance not active or not running	A request has been made of the LLC layer, but the MAC instance is not active and running. As a result, the LLC layer is unable to process the request. This completion code can be returned for any of the LLC primitives.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
7606	SAPs still active	This completion code is returned on the DL_ENABLE confirm primitive. The LLC layer received a request to disable the layer, but all the SAPs have not been closed.
7607	Layer enabled successfully	This completion code is returned in response to a DL_ENABLE request that completes successfully. This completion code is returned by LLC when the LLC layer is successfully enabled. It implies that the MAC layer was successfully enabled.
7608	Layer already enabled	This completion code is returned in response to a DL_ENABLE request, and does not indicate an error situation. The LLC received an ENABLE request, but the layer was already enabled.
7609	Station already opened	This completion code is returned in response to a DL_OPEN_STN request. It indicates that the station requested to be open has already been opened.
760A	New route for station	This completion code is returned in response to a DL_OPEN_STN request, DL_REQ_OPNSTN request, and DL_CONNECT request.
760B	Link disconnected; transmission retry count, N2, exceeded	This completion code is returned in response to a DL_DISCONNECT request. It indicates that the LLC layer tried to disconnect the link in an orderly fashion but could not get a response from the remote station. See the *IBM Token-Ring Network Architecture Reference* for information on the maximum number of transmissions, N2.
760C	Remote station in busy state	This completion code is returned in response to a DL_DATA request. It informs the user to temporarily stop sending data to the remote station until the busy condition is removed.
760D	Remote station in ready state	This completion code is returned in response to a DL_DATA request. It informs the user that the remote station is no longer in a busy state and that data may now be forwarded to the station.
760E	Mismatched XID type	This completion code is returned in response to a DL_ID request. It indicates that the XID returned in response to the request is of a different type. The XID data received in response is returned with this code in the DL_ID confirm.
760F	Link disconnected, DISCONNECT received	This completion code is returned in response to a DL_DATA request. It indicates that a DISCONNECT command was received from the remote station when the local station was processing the DL_DATA request. The receipt of the frame associated with the DL_DATA request is not guaranteed.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
7610	Link disconnected, Disconnected Mode Response received	This completion code is returned in response to either a DL_CONNECT request or a DL_DATA request. It indicates, respectively, that the remote station has rejected the DL_CONNECT request or that the remote station is in disconnected mode, respectively.
7611	SAP deactivated	This completion code is returned in response to a DL_DEACTIVATE_SAP request. It indicates that the SAP was successfully deactivated.
7612	MAC_type not valid	This completion code is returned in response to a DL_ENABLE request. It indicates that the MAC_type specified in the primitive does not match any of the defined MAC types.
7613	LLC_instance name not valid	This completion code is returned in response to a DL_ENABLE request. It indicates that the LLC_instance name specified in the primitive is not valid.
7614	Maximum LPDU size too large	This completion code is returned in response to a DL_ENABLE request. It indicates that the LPDU size requested is larger than the LLC or MAC can support.
7615	LLC layer not enabled	This completion code is returned in response to a DL_DISABLE or DL_ACTIVATE_SAP request. For the DL_DISABLE request it indicates that the LLC layer was not enabled when the request was received. For the DL_ACTIVATE_SAP request, it indicates that the LLC layer was not enabled as is necessary before activating an SAP.
7616	LSAP already in use	This completion code is returned in response to a DL_ACTIVATE_SAP request. The request is rejected because the SAP is already activated.
7617	Aborted by DL_DEACTIVATE_SAP	This completion code is returned in response to DL_ACTIVATE_SAP, DL_MODIFY_SAP, DL_OPEN_STN, DL_CLOSE_STN, DL_REQ_OPNSTN, DL_ID, DL_CONNECT, DL_DISCONNECT, DL_DATA, and DL_MSG requests. It indicates that the request could not be processed before the receipt of a DL_DEACTIVATE_SAP requesting the deactivation of the SAP on which the request was being processed.
7618	LLC_SAP_name not valid	This completion code is returned in response to a DL_ACTIVATE_SAP request. It indicates that the LLC_SAP_name in the request was not valid.
7619	SAP ID not found SAP not activated	This completion code is returned in response to DL_MODIFY_SAP, DL_DEACTIVATE_SAP, DL_OPEN_STN, DL_CLOSE_STN, DL_REQ_OPNSTN, and DL_MSG requests.
761A	LSAP address not valid	This completion code is returned in response to a DL_ACTIVATE_SAP request. It indicates that the request was rejected because the LSAP address provided with the primitive was not valid.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
761B	SAP ID not found	This completion code is returned in response to DL_OPEN_STN, DL_MODIFY_STN, DL_CLOSE_STN, DL_REQ_OPNSTN, DL_RTV_ATTRIB, DL_ID, DL_CONNECT, DL_DISCONNECT, DL_DATA, and DL_FLOW requests. It indicates that the SAP referenced in the request was not found. As a result, the request is rejected.
761C	Station_name not valid	This completion code is returned in response to DL_OPEN_STATION and DL_REQ_OPNSTN requests. It indicates that the station name specified in the primitive is not valid.
761D	DSAP not valid	This completion code is returned in response to DL_OPEN_STN, DL_REQ_OPNSTN, and DL_MSG requests. It indicates that the DSAP specified in the primitive is not valid.
761E	Class_of_service not valid	This completion code is returned in response to DL_ENABLE and DL_ACTIVATE_SAP requests. It indicates that the class of service requested in the primitive was not valid.
761F	MAC SAP name not valid	This completion code is returned in response to a DL_ENABLE request. It indicates that the MAC SAP name specified in the primitive is not valid.
7620	MAC_instance name not valid	This completion code is returned in response to a DL_ENABLE request. It indicates that the MAC instance name specified in the primitive is not valid.
7621	MAC enable parameter not valid	This completion code is returned in response to a DL_ENABLE request. It indicates that one of the MAC enable parameters is not valid.
7622	MAC SAP parameter not valid	This completion code is returned in response to DL_ENABLE, DL_ACTIVATE_SAP, and DL_MODIFY_SAP requests. It indicates that the one of the MAC SAP parameters is not valid.
7623	LSAP_type not valid	This completion code is returned in response to a DL_ACTIVATE_SAP request. It indicates that the LSAP type is not valid because it is not type 802.2, SNA, or IMPL server.
7624	Aborted by DL_DISCONNECT	This completion code is returned in response to a DL_DATA request. It indicates that the connection was disconnected prior to completion of the request to send data.
7625	Data_length exceeded maximum LPDU size	This completion code is returned in response to DL_DATA and DL_MSG requests. It indicates that the PDU size request is larger than the maximum LPDU size. The request is rejected.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
7626	Link station not in connected state	This completion code is returned in response to DL_DATA and DL_FLOW requests. These requests require an established link station and a virtual link to the remote station. The request is rejected.
7627	Link_Error_ Recovery_Option not valid	This completion code is returned in response to DL_OPEN_STN, DL_MODIFY_STN, and DL_REQ_OPNSTN requests. It indicates that the link-error-recovery option specified in the primitive is not valid.
7628	Send_Window_Size not valid	This completion code is returned in response to DL_OPEN_STN, DL_MODIFY_STN, and DL_REQ_OPNSTN requests. It indicates that the send-window size specified in the primitive is not valid.
7629	ACK frequency, N3 not valid	This completion code is returned in response to DL_OPEN_STN, DL_MODIFY_STN, and DL_REQ_OPNSTN requests. It indicates that the send value specified for N3 in the primitive is not valid. See the *IBM Token-Ring Network Architecture Reference* for information on acknowledgement frequency, N3.
762A	Dynamic window option not valid	This completion code is returned in response to DL_OPEN_STN, DL_MODIFY_STN, and DL_REQ_OPNSTN requests. It indicates that the value for the dynamic-window option specified in the primitive is not valid.
762B	Window step not valid	This completion code is returned in response to DL_OPEN_STN, DL_MODIFY_STN, and DL_REQ_OPNSTN requests. It indicates that the value of the window-step parameter specified in the primitive is not valid.
762C	Length-of-route field not valid	This completion code is returned in response to DL_OPEN_STN, DL_MODIFY_STN, and DL_REQ_OPNSTN requests. It indicates that the length specified for the routing information field is not valid.
762D	Route not modified (station in connected state)	This completion code is returned in response to a DL_MODIFY_STN request. It indicates that because the station has a Type 2 connection established with a remote station, the route cannot be changed. The request to change the route is rejected.
762E	Station of specified SAP ID not found	This completion code is returned in response to a DL_CLOSE_STN request. It indicates that the SAP identifier requested to be closed does not exist according to the LLC layer.
762F	XID type not valid	This completion code is returned in response to a DL_ID request. It indicates that the XID type specified in the request was not known to the LLC layer.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
7630	DL_CONNECT outstanding	DL_DISCONNECT request cannot be processed at this time because the connect request is still in process. The disconnect command is rejected.
7631	DL_DISCONNECT outstanding	DL_CONNECT request cannot be processed at this time because a disconnect request is still in process. The connect command is rejected.
7632	DL_SIM outstanding	DL_CONNECT request or DL_DISCONNECT request cannot be processed at this time because the SIM request is still in process.
7633	Previous XID request outstanding	This completion code is returned in response to a DL_ID request. It indicates that a request to send an XID has not yet been completed. Only one XID request may be in process at a time.
7634	Requested class of service not supported	This completion code is returned in response to DL_ENABLE and DL_ACTIVATE_SAP requests. It indicates that the class of service specified is not supported by the LLC entity. The request is rejected.
7635	Class_of_service not valid	This completion code is returned in response to DL_ENABLE and DL_ACTIVATE_SAP requests. It indicates that the class of service requested in the primitive was not valid.
7636	Aborted by DL_CLOSE_STN	This completion code is returned in response to DL_OPEN_STN, DL_REQ_OPNSTN, DL_ID, DL_CONNECT, DL_DISCONNECT, and DL_DATA requests. It indicates that a Close Station was received before completing the processing of the request. The request is aborted.
7637	Failure to disable MAC instance	This completion code is returned in response to a DL_DISABLE request. In order to disable the LLC layer, the MAC layer must be disabled. This code indicates that there was a problem in disabling the MAC layer.
7638	MAC_ENABLE failed, no resource	This completion code is returned in response to a DL_ENABLE request. A MAC_ENABLE request was passed to MAC by LLC as a result of the DL_ENABLE request. The MAC_ENABLE request failed due to a lack of resource.
7639	MAC_ACTIVATE_SAP failed, no resource	This completion code is returned in response to a DL_ENABLE request. A MAC_ACTIVATE_SAP request was passed to MAC by LLC as a result of the DL_ACTIVATE_SAP request. The MAC_ACTIVATE_SAP request failed due to a lack of resource.
763A	Resource not available	This completion code is returned in response to a DL_ENABLE, DL_ACTIVATE_SAP, DL_OPEN_STN, and DL_REQ_OPNSTN requests. This code indicates that a resource needed to complete the request was not available.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
763B	Route_Resolve failed	This completion code is returned in response to DL_OPEN_STN and DL_REQ_OPNSTN requests. This code indicates that the LLC layer was unable to determine a route through the network to the remote station.
763C	Link disconnected; transmission retry count, N2, exceeded	This completion code is returned in response to DL_CONNECT and DL_DATA requests. It indicates that the LLC layer tried to send the necessary PDU for the request but exhausted the retries. See the *IBM Token-Ring Network Architecture Reference* for information on the maximum number of transmissions, N2.
763D	Link resetting (FRMR sent out)	This completion code is returned in response to a DL_DATA request. The LLC layer detected a need to reset the link and sent a frame-reject to the remote station. The request is rejected.
763E	Link resetting (FRMR received, SABME being sent)	This completion code is returned in response to a DL_DATA request. The remote LLC detected a need to reset the link and sent a frame-reject. The local LLC responded with a SABME to reset the link. The request is rejected.
763F	Link resetting (FRMR received, DISC being sent)	This completion code is returned in response to a DL_DATA request. The remote LLC detected a need to reset the link and sent a frame-reject. The local LLC responded with a DISC to terminate the link. The request is rejected.
7641	Required parameter(s) not provided	This completion code is returned if one or more of the required parameters for this primitive for which no default is available is coded as zero.
7642	Option(s) not valid or incompatible	The options specified in the parameter data field are not a valid combination, for example, an attempt is made to open an SAP that has an XID handling option different from that of the group SAP with which it is associated.
7643	Command canceled due to unrecoverable failure	This completion code is returned when a command causes an unrecoverable failure of the adapter.
7644	Unauthorized access priority	This completion code is returned if an incorrect access priority was requested from an activate_SAP or modify_SAP request.
7645	Command canceled, adapter was not enabled	This completion code is returned if the adapter specified in the command was never enabled.
7646	Command canceled, adapter closed while command in process	This completion code is returned if the adapter was closed while the command was in process. This could be due to an error condition, or to the receipt of a deactivate_subsystem request being received.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
7647	Adapter already enabled	This completion code is returned on the adapter_enable confirm when the target adapter has already been enabled by another user. This code does not indicate an error situation.
7648	Adapter already enabled	This completion code is returned on the adapter_enable confirm when the target adapter has already been enabled by this user. This code indicates an error.
7649	Adapter already disabled	This completion code is returned on the adapter_disable confirm when the target adapter has already been disabled by this user. This code indicates an error.
764A	Adapter not enabled	This completion code is returned on the adapter_enable confirm when the target adapter cannot be enabled due to either a load failure or a hardware failure. This code indicates an error situation.
764B	Adapter value not valid	This completion code is returned if any primitive is received for an adapter that is not present.
764B	Invalid adapter value	This completion code is returned on any command targeted for an adapter that was not explicitly enabled by this user.
764D	Error on frame transmission	This completion code is returned on a Type I data transmission confirm if the receiving adapter did not copy the data frame from the token-ring network.
764F	Error in frame transmit or strip process	This completion code is returned on a Type I data transmission confirm if an error was detected by the adapter either during frame transmission or when the frame was read back and checked.
7650	FRMR response received	Upon receipt of the FRMR response, the local LLC service provider has sent a RESET indication (local) to the LLC user.
7651	Timer expired and retry exhausted	A time-out condition has occurred, and the retry count is exhausted. The local LLC service provider has sent a RESET indication (local) to the LLC user.
7652	SABME received	The remote LLC has sent a SABME to the local LLC. The local LLC service provider has sent a RESET indication (remote) to the LLC user. etable.
7653	Link not transmitting I-frames State changed from link-opened	This completion code is returned on a LLC_DATA request if the link station leaves the link-opened state due to a received frame (such as DISC) or a timeout.
7655	Disconnected Mode Response received	This completion code is returned on the close_station_indication. It indicates the reason the LLC service provider issued the request.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
7656	DISC received	This completion code is returned on the close_station_indication and provides the reason the LLC service provider issued the request. For example, this code is returned when a 3172 receives a Disconnect from a PC.
7657	Link connection INOP	This completion code is returned on the close_station_indication and provides the reason the LLC service provider issued the request.
7658	Parameter exceeded maximum allowed	This completion code is a returned when a required parameter in the primitive data field exceeded the maximum allowed value. Try again with a valid value.
7659	Requested membership in non-existent group SAP	This completion code is returned if an activate_SAP or modify_SAP request is received, requesting membership in a group SAP that does not exist. See the *IBM Token-Ring Network Architecture Reference* information on the group SAP.
765C	Group SAP has reached maximum membership	This completion code is returned if an activate_SAP or modify_SAP request is received, requesting membership in a group SAP that has reached its maximum membership. The command completes up to the point at which the error was encountered. Other parameters have been changed if the request was modify_SAP. See the *IBM Token-Ring Network Architecture Reference* for information on the group SAP.
765E	Member SAP not found in group SAP list	This completion code is returned if a Modify_SAP request is received, requesting deletion of the member SAP from a group SAP of which it was not a member. The command completes up to the point at which the adapter encountered the error. Other parameters have been modified as requested. See the *IBM Token-Ring Network Architecture Reference* for information on the group SAP.
FF02	Duplicate command	This completion code is returned if a connect request is received for a link station, while a previous connect request is still in process.
FF0C	Command cancelled, version number not valid	This completion code is returned if the primitive contained a version number that was not valid.
FF28	Duplicate LLC request	This completion code is returned on a DL_DATA or DL_REPLY when a duplicate request with the same source SAP, destination MAC, and priority is received by the LLC service provider.
FF48	Group SAP cannot close, all member SAPs not closed	This completion code is returned if a deactivate_SAP request is received for a group SAP while members of that group SAP are still open. Close the members and try the deactivate_SAP request again.

Table 8. LLC LAN specific codes (continued)

Code	Meaning	Explanation
FF4C	Sequence error	This completion code is returned if a deactivate_SAP or close request is received while other SAP or link commands are still in process. Wait for the commands to complete and re-issue the close request.
FF4F	Invalid remote address	This completion code is returned if an OPEN_STATION request is received with the remote MAC address parameter high bit of the high byte set to one. This indicates a group address. A group address is not allowed to be specified for this command. **VTAM hint:** A possible cause of code FF4F is that DLCADDR is specified in the definition for a 3172. The 3172 does not currently support DLCADDR. DLCADDR is a parameter on the PATH definition statement for a switched major node.
FF50	Attribute value; no values set not valid	This completion code is returned indicating that none of the requested attribute modifications were made.
FF51	Attributes values; one or more values set not valid	This completion code is returned indicating partial completion of the requested attribute modifications.
FF52	One or more requested attributes not available	This completion code is returned indicating some of the requested attribute values were not available.
FF53	DL_Flow option not valid	This completion code is returned if the user specifies flow off when it is already off or flow on when it is already on.
FF76	A frame reject (FRMR) was sent to the DSPU	The FRMR sent is the result of one of the following reasons: • MAC frame control field not valid • I-field contains data that is not valid for that control field included in a SABME • The received I-field length exceeds the buffer • LPDU control field sequence number error • The FRMR response I-field is not five bytes in length

Chapter 3. Data link control (DLC) status codes

DLC status codes provide information about errors that are encountered during the use of high performance data transfer (HPDT) and z/OS Container Extensions on z/OS Direct Network Interface (DNI) services. They are displayed in some messages and in the IUTx and DNIx VIT entries.

DLC status codes are 4 bytes long. The bytes contain the following information:

Byte
Contents

0
Category

1
Reporting layer identifier and location

2 and 3
Completion code

The following tables show the possible values that can appear in each byte and their meaning.

Table 9. Byte 0 (category) of the DLC status code

Hexadecimal Value	Meaning
X'00'	Request successful **Explanation:** The specific request has been processed with no error. The receiver of this request successfully forwarded or replied to this request. **Note:** The completion code could have informational errors.
X'08'	Request rejected **Explanation:** All aspects of the request were understood but a transitory system or network error occurred which prevented the execution of this request. An example of this could be storage shortage. **Note:** This category is one that an upper layer protocol (ULP) might choose to try the failed primitive again.
X'10'	Request error **Explanation:** This request was rejected due to inaccurate information in the primitive (for example, incorrect token, incorrect information element).
X'20'	State error **Explanation:** A request was received "out of order."
X'40'	Usage error **Explanation:** Request rejected due to incorrect use of either the request itself or a parameter that is associated with the request.
X'80'	Permanent error **Explanation:** Request rejected due to failure of either a system or network function.

© Copyright IBM Corp. 2000, 2021

Table 10. Byte 1 (reporting layer identifier and location) of the DLC status code	
Hexadecimal Value	**Meaning**
X'10'	LLC or DNI layer local error **Explanation:** A request was processed and an error was found by the local VTAM.
X'20'	LLC layer path error **Explanation:** A request was processed and an error was found by the local VTAM while trying to send a primitive out on an MPC group.
X'30'	LLC or DNI layer remote error **Explanation:** A request was processed and an error was found by the remote VTAM. This value should be used when a remote VTAM is sending common status back to an adjacent host.
X'12'	Port Control Manager (PCM) local error **Explanation:** A primitive was processed and an error was found by the IBM Open System Adapter's PCM.
X'22'	Port Control Manager path-related error **Explanation:** A primitive was processed and an error was found by the IBM Open System Adapter's PCM while trying to send a primitive out on an MPC group or sending a primitive to the ATM network.
X'32'	Port Control Manager remote error **Explanation:** A primitive was processed and an error was found by the remote node; for example, the local ATM switch experienced a failure.
X'1C'	Service-specific component local error **Explanation:** A primitive was processed and an error was found by a service-specific component part of the ATM adaptation layer (AAL) sublayer.
X'2C'	Service-specific component path-related error **Explanation:** A primitive was processed and an error was found by a service-specific component part of the AAL sublayer, while trying to send a primitive to the ATM network.
X'3C'	Service-specific component remote error **Explanation:** A primitive was processed and an error was found by the remote node; for example, the local ATM switch experienced a failure.
X'1A'	Common-part component local error **Explanation:** A primitive was processed and an error was found by a common-part component that includes the ATM layer function and non-service-specific sublayers of the AAL layer.
X'2A'	Common-part component path-related error **Explanation:** A primitive was processed and an error was found by a common-part component that includes the ATM layer function and non-service-specific sublayers of the AAL layer while trying to send a primitive to the ATM network.

Table 10. Byte 1 (reporting layer identifier and location) of the DLC status code (continued)	
Hexadecimal Value	**Meaning**
X'3A'	Common-part component remote error **Explanation:** A primitive was processed and an error was found by a remote partner in its common-part component that includes the ATM layer function and non-service-specific sublayers of the AAL layer.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code	
Hexadecimal Code	**Meaning**
X'00nn'	n/a **Explanation:** Codes starting with X'00' are specific to the VTAM product implementation.
X'0000'	Successful **Explanation:** The primitive completed successfully.
X'0001'	Initialization failure **Explanation:** A failure occurred during the initialization of support code. Notify VTAM operator to determine cause of failure.
X'0018'	VTAM is not available **Explanation:** Request returned as a result of VTAM termination. Termination might be normal due to an operator initiated action or due to some abnormal condition.
X'0021'	Connection constructor error **Explanation:** Failure occurred during the construction of the connection object. Notify the VTAM operator of the failure to determine cause and possible corrective actions.
X'0022'	State error **Explanation:** Failure occurred during the execution of the request due to a state error indicating a protocol violation. Notify the VTAM operator of the failure to determine cause of inconsistency and possible corrective actions.
X'0023'	TRLE activation/deactivation state error **Explanation:** User issued an activate or deactivation request and an internal state error was encountered.
X'0024'	Provider ID error **Explanation:** Provider ID supplied on the primitive is either incorrect or cannot be found. Condition indicates an interface inconsistency. Notify the VTAM operator of the failure to determine cause of inconsistency and possible corrective actions.
X'0025'	Selective Retransmit Not Supported **Explanation:** A request to set up a connection was received, and Selective Retransmit service was requested for that connection. Selective Retransmit is not supported now, so the request was rejected. Condition indicates that the remote partner expects Selective Retransmit, which might be a configuration mismatch. Notify the VTAM operator of the failure to determine cause of inconsistency and possible corrective actions.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'0027'	OpenPathReq error **Explanation:** Internal command OPENPATH_request, which causes the initial activation of the channel paths and either the XID or IDX exchange, failed. Failure might be due to a channel problem or an error condition that is discovered during the initial activation sequence. Notify the VTAM operator of the failure to determine cause and possible corrective actions. It might also be necessary to notify the operator of the platform containing the remote MPC instance.
X'0029'	DactPathReq error **Explanation:** Internal command DACTPATH_request, which causes the termination of an MPC group, failed for some reason. MPC will complete system takedown of the group but the user should notify the VTAM operator of the failure to determine cause and possible corrective actions. Failure to take corrective action might lead to the inability to reactivate the path.
X'002A'	ActPathRsp error **Explanation:** Internal command ACTPATH_response, which causes the allocation of devices and the construction of the MPC environment, failed. Notify the VTAM operator of the failure to determine cause and possible corrective actions.
X'002B'	OpenPathRsp error **Explanation:** Internal command OPENPATH_response, which causes the initial activation of the channel paths and either the XID or IDX exchange, failed. Failure might be due to a channel problem or an error condition that is discovered during the initial activation sequence. Notify the VTAM operator of the failure to determine cause and possible corrective actions. It might also be necessary to notify the operator of the platform containing the remote MPC instance.
X'002F'	MPC connection does not support high performance data transfer. **Explanation:** Either the local definitions or the remote partner does not support high performance data transfer data interface. Check Hardware Configuration Definition (HCD) and VTAM definitions for possible mismatch.
X'0030'	Storage error **Explanation:** Storage incorrect or not obtainable.
X'0040'	INOP-deact SAP **Explanation:** SAP becomes inoperative.
X'0041'	INOP-connection **Explanation:** Data connection becomes inoperative.
X'0042'	INOP-signaling connection **Explanation:** Signaling connection becomes inoperative.
X'0043'	INOP-device **Explanation:** Local device becomes inoperative.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'0044'	INOP-soft **Explanation:** The connection or MPC group is inoperative; however, recovery of the connection is possible.
X'0045'	INOP-hard **Explanation:** The connection or MPC group is inoperative, and is not expected to recover without intervention.
X'0046'	Incorrect token **Explanation:** User specified an incorrect token on a data connection.
X'0047'	Incorrect token **Explanation:** Internally specified token incorrect.
X'0048'	Duplicate data activation request **Explanation:** ULP has sent multiple data activation requests for a single connection.
X'0049'	Selector value error **Explanation:** A primitive was processed that specified a selector that did not match the selector of the provider token that was received.
X'004A'	Protocol value error **Explanation:** A primitive was processed that did not specify a known protocol value.
X'004B'	VCNAME value error **Explanation:** A primitive was processed that did not specify a known virtual circuit value.
X'0050'	Multiple TCP/IP instances trying to register filters for incoming calls **Explanation:** Multiple TCP/IPs requested identical filter values.
X'0051'	Buffer size error **Explanation:** An activation SAP request was issued with an incorrect bufsize, or an incorrect combination of buffer size and buffer number for a TCP/IP read or write device.
X'0052'	Missing XBFL **Explanation:** An attempt was made to execute a data primitive and an XBFL (extended buffer list) was not provided. An XBFL is required for data primitives.
X'0053'	Empty XBFL **Explanation:** An XBFL was provided for a data primitive that has no entries within the list; for example, XBFLBEGN=0.
X'0054'	Incorrect XBFL entry **Explanation:** An XBFL was provided for a data primitive that has an incorrect entry within the list (for example, XBFLAREA=0).

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'0055'	Packet and XBFL length mismatch **Explanation:** An XBFL was provided for a data primitive where the total length of all entries does not match the packet length.
X'0056'	XBFL free option not specified **Explanation:** An XBFL was provided for a data primitive where the XBFL free option (XBFL_FREE_OPT) was not specified. The free option is required for all data primitives.
X'0057'	Incorrect packet length **Explanation:** The packet length was 0 or too large; for example, exceeds the defined values for the device.
X'0058'	Incorrect parameter list version **Explanation:** The parameter list version is incorrect.
X'0060'	Connection not active **Explanation:** The data activation request for a specific connection was received before the connection was active.
X'0061'	Data not enabled with data activation request **Explanation:** Data activation request has not been received so data cannot be processed.
X'0062'	Class value error **Explanation:** A primitive was processed that does not specify a known class value.
X'0063'	Control value error **Explanation:** A primitive was processed that does not specify a known control value which is permitted for this primitive.
X'0064'	MPC Group in Use **Explanation:** An MPC group is defined as EXCLUSIVE USE (MPCUSAGE = EXC on TRLE), and is already in use. Activation is rejected.
X'0065'	iQDIO Prohibited **Explanation:** iQDIO activation is prohibited by VTAM start option IQDCHPID = NONE.
X'0066'	iQDIO CHPID Ambiguous **Explanation:** iQDIO activation is not allowed due to an ambiguous configuration with specifying IQDCHPID = ANY (default), and configuring (HCD/IOCDS) multiple IQD CHPIDs to this logical partition (LPAR). When IQDCHPID = ANY is specified (or defaulted) only one IQD CHPID can be configured for this LPAR. If multiple IQD CHPIDs must be configured to this LPAR, then define IQDCHPID = 'HEXCHPID' (the specific hex IQDCHPID that this LPAR should use).

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'0067'	iQDIO or QDIO Devices Not Available **Explanation:** An attempt was made to build a dynamic TRLE for a QDIO OSA-Express device or a HiperSockets device, but VTAM could not find the minimum number of required subchannel devices (CUAs) for the device. For a HiperSockets device, at least 3 CUAs are required to the same HiperSockets CHPID. For a QDIO OSA-Express device, the OSA-Express CHPID must be configured with 2 consecutive device addresses beginning with an even number for the control channels, and at least one additional device address for a DATAPATH channel. Verify the HCD or IOCDS configuration for accuracy for this logical partition (LPAR).
X'0068'	iQDIO CHPID Conflict **Explanation:** The user defined an iQDIO device CHPID and it conflicts with the sysplex IQD CHPID. This is defined by the IQDCHPID start option and is used for DYNAMICXCF communication. For more information, see the IQDCHPID start option in z/OS Communications Server: SNA Resource Definition Reference.
X'0069'	Processor not iQDIO capable **Explanation:** The user attempted to activate an iQDIO device and the processor does not support iQDIO devices.
X'006A'	iQDIO IQD CHPID multiple channel subsystem error **Explanation:** Multiple channel subsystem capable machine but the Internal Channel ID (CHID) is not available.
X'006B'	Frame invalidation mismatch **Explanation:** Frame invalidation is not supported by the stack that is issuing ActSap and frame invalidation was enabled by the first stack to issue ActSap.
X'006C'	Too many input queues requested by the stack **Explanation:** The stack specified more input queues than supported.
X'006D'	Input queue ID out of range **Explanation:** An internal Communications Server error occurred.
X'006E'	Input queue ID not registered **Explanation:** An internal Communications Server error occurred.
X'006F'	QDIO or IQDIO CHPID Not Available **Explanation:** An attempt was made to build a dynamic TRLE for a QDIO OSA-Express device or a HiperSockets device, and a CHPID for this device could not be found. If the CHPID was configured, for example on an MPCIPA HiperSockets device statement or using the CHPID parameter on an OSA-Express QDIO Interface statement, that particular CHPID was not defined to the system. If the CHPID was searched for dynamically, for example activating a dynamic IUTIQDIO link for HiperSockets with VTAM start option IQDCHPID=ANY or an OSA-Express OSM device, a CHPID for that particular channel type was not defined to the system. Verify the configured CHPID parameter or the HCD or IOCDS configuration for accuracy for this logical partition (LPAR).

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'0070'	QDIO device control channels not available **Explanation:** An attempt was made to build a dynamic TRLE for a QDIO OSA-Express device. A CHPID was found, but two consecutively numbered device addresses beginning with an even number could not be found. For QDIO OSA-Express devices, an even-numbered device address is required for the READ control channel, and the next consecutive odd address for the WRITE control channel. Verify the HCD or IOCDS configuration for accuracy for this logical partition (LPAR).
X'30nn'	n/a **Explanation:** Codes starting with X'30' can be errors that are detected in the interface between TCP/IP and VTAM, between VTAM and the IBM Open System Adapter, or between VTAM and TCP/IP channel units. These errors result from either a software or definitional problem. Use the specific return code to help identify the problem.
X'3001'	Incorrect control information field **Explanation:** The control information field of the primitive contains data that is blank, in an incorrect format, or cannot be recognized.
X'3002'	Incorrect identifier **Explanation:** The value that is specified in the identifier/token parameter of the control information field is blank, in an incorrect format, or cannot be recognized.
X'3003'	Incorrect identifier type **Explanation:** The value that is specified in the identifier type parameter of the control information field is incorrect; for example, the ID type says it is an SAP but the identifier is a filter.
X'3004'	Incorrect primitive **Explanation:** The value that is specified in the primitive code parameter of the control information field is incorrect.
X'3005'	State error **Explanation:** An illogical or incorrect primitive was received for the current SAP or the call instance state of the Port Connection Manager.
X'3007'	Incorrect information data **Explanation:** Either the primitive's data information field is missing data, or it contains blank, syntactically incorrect, or unrecognizable data.
X'3008'	Resource not available **Explanation:** The requested resource is not available.
X'300A'	Task ABEND **Explanation:** An error occurred that prevents the processing of the primitive.
X'300E'	Incorrect service type **Explanation:** The ServiceType parameter in the primitive's Control Information field is either blank, syntactically incorrect, or unrecognizable. Service Type is REQ/CNF/IND/RSP.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'3011'	IBM Open Systems Adapter disabled **Explanation:** The IBM Open Systems Adapter has been disabled by user command.
X'3012'	PVC removed from IBM Open Systems Adapter **Explanation:** A PVC definition has been removed from IBM Open Systems Adapter while that PVC connection was active. The PVC connection is being deactivated.
X'3013'	PCM signaling virtual channel is not active **Explanation:** The signaling virtual channel (VCI=5, VPCI=0) between the IBM Open Systems Adapter and the ATM switch that carries signaling requests is not active.
X'3014'	Incorrect entry point **Explanation:** The entry point/interpret routine indicated contains a null character or incorrect value.
X'3016'	Incorrect Port Control Manager name **Explanation:** The value that is specified in the Port Control Manager name parameter is blank, in an incorrect format, or cannot be recognized. **Note:** 1. The port name is specified in multiple places and **MUST** be the same in the IBM Open Systems Adapter/SF configuration file, on the PORTNAME operand on the TRLE definition statement in the TRL major node, and (in the case of APPN communication) on the PORTNAME operand on the PORT definition statement in the XCA major node. The port name must be the same in all places that it is specified. If it is not, correct the mismatches. 2. The user request is failed if the requested TRLE cannot be activated because of one of the following conditions. • TRL major node has not been activated. • The TRLE entry is missing from the activated TRL major node. • The TRLE entry has an error that does not allow it to be defined. • The TRLE has been activated but it is inoperative.
X'3017'	Incorrect user call instance identifier **Explanation:** The value that is specified in the user call instance identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'3018'	Incorrect provider call instance identifier **Explanation:** The value that is specified in the provider call instance identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'3019'	Incorrect user SAP identifier **Explanation:** The value that is specified in the user SAP identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'301A'	Incorrect provider SAP identifier **Explanation:** The value that is specified in the provider SAP identifier parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'301B'	Incorrect provider call enabling identifier **Explanation:** The value that is specified in the P_CE_ID parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'301C'	Incorrect user call enabling identifier **Explanation:** The value that is specified in the U_CE_ID parameter of the control information field is missing, blank, in an incorrect format, or cannot be recognized.
X'3022'	Incorrect control information field length **Explanation:** The value that is specified in the control information field length parameter contains an incorrect value. **Note:** Each primitive has a unique fixed control information field.
X'3023'	Incorrect data information field length **Explanation:** The value that is specified in the data information field length parameter contains a value that is incorrect or unrecognized.
X'3024'	Incorrect action code **Explanation:** The value that is specified in the action code specified in the control information on the Call_Setup response field is missing, blank, in an incorrect format, or cannot be recognized.
X'3025'	Missing data information field **Explanation:** The data information field must be complete for the primitive to work.
X'3026'	Incorrect logical link value **Explanation:** The value that is specified in the logical link identifier parameter is outside the valid range of 0-31, decimal.
X'3027'	PCM TRLE cannot support selector **Explanation:** The user issued an activate request that specified a selector that is not valid for the TRLE found by RNAME.
X'3028'	Datapath device activation failed **Explanation:** A storage error occurred during early processing of a datapath channel address for a QDIO device.
X'3029'	Datapath device activation negative **Explanation:** An error occurred attempting to allocate or activate a datapath channel address for a QDIO device.
X'302A'	Datapath device Open failed **Explanation:** An error occurred attempting to start a connection across a datapath channel address for a QDIO device.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'302B'	Datapath Device Start Data failed **Explanation:** An error occurred attempting to start data flow on a connection across a datapath channel address for a QDIO device.
X'302C'	Enable Incoming connections for Port failed **Explanation:** A QDIO device rejected an attempt to allow connections to be enabled on this device.
X'302D'	No datapath devices available **Explanation:** A ULP cannot use a QDIO device because there are no datapath channel addresses available.
X'302E'	Activation failed to complete **Explanation:** A QDIO or iQDIO device failed to complete activation or properly register its HOME IP Address within 5 minutes.
X'302F'	Channel unit address not available **Explanation:** The channel is not the correct type for this device, there is no path for this channel, or the channel is not varied online.
X'3030'	Incorrect channel unit address specification **Explanation:** The channel unit address was either not specified by TCP/IP or is not a correct hexadecimal number.
X'3031'	Channel unit address already in use **Explanation:** The channel unit address specified by TCP/IP is already allocated to another user.
X'3032'	Maximum connections exceeded **Explanation:** The connection request attempted for this device exceeds the allowable maximum for this device type.
X'3033'	Lack of resources **Explanation:** The resources requested from the system could not be obtained (for example, memory errors).
X'3034'	Connection failed by the remote host with no cause code **Explanation:** A connection request was failed by the remote host for a given device, but a cause code indicating why the connection failed was not supplied.
X'3035'	QDIO CHPID type mismatch **Explanation:** An attempt was made to activate a QDIO device for a particular CHPID type, but the TRLE associated with this device was already active with channels of a different CHPID type. Verify the DEVICE name or PORTNAME are correctly configured for this device, and if the TRLE was configured, verify the device addresses are addresses for a CHPID of the correct type.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'3036'	Secondary OSM Interface activated before primary **Explanation:** An attempt was made to activate EZ6OSM02 before EZ6OSM01. This failure can occur when there are no OSM CHPIDs available at TCP/IP stack initialization, and EZ6OSM02 is subsequently activated before EZ6OSM01. Activate EZ6OSM01 then EZ6OSM02.
X'3037'	OSX or OSM Interface activation not permitted **Explanation:** An attempt was made to activate an interface with CHPID type OSX or OSM. The activation attempt failed because the ENSEMBLE start option is set to NO, which does not permit TCP/IP connectivity to either the intraensemble data network or the intranode management network.
X'3038'	OSX or OSM Interface activation not permitted **Explanation:** An attempt was made to activate an interface with CHPID type OSX or OSM. The activation attempt failed because the central processor complex (CPC) is not configured as a member of an ensemble.
X'3039'	IQD activation not permitted against an IQDX device **Explanation:** A CHPID that is defined to HCD as IQDX cannot be used as an iQDIO device.
X'303A'	Function type not valid **Explanation:** The "RoCE Express" interface does not recognize the function identifier on the activation attempt.
X'303B'	Outbound request flood detected **Explanation:** The Internet Control Message Protocol (ICMP) time stamp request is rejected because CSM storage is constrained or too many time stamp requests are generated at the same time.
X'303C'	IQD activation not permitted against an IQDC device **Explanation:** An IQD CHPID that is defined to HCD with an external function type of External Bridge cannot be used as a Layer 3 iQDIO device.
X'3053'	Maximum number of network interfaces exceeded **Explanation:** An attempt was made to activate an OSA-Express port in QDIO mode. The OSA-Express port, or another port on the same OSA-Express3 or later channel path identifier (CHPID), is currently operating in optimized latency mode for at least one network interface. Optimized latency mode limits the number of concurrent network interfaces allowed to share this port and this CHPID. This activation attempt exceeds that limit. See the information about the optimized latency mode in z/OS Communications Server: IP Configuration Guide for information about these limits.
X'31nn'	OSA-Express rejected an attempt to activate a port **Explanation:** Codes starting with X'31' are specific to OSA-Express QDIO Mode activation attempts. X'31' indicates that the OSA has rejected an activation attempt. The *nn* indicates the reason for the rejection. Specific *nn* codes are listed in this table. If you receive a code that is not listed in this table, contact IBM Service.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'311B'	Duplicate port name **Explanation:** An attempt was made to activate an OSA-Express3 or later port in QDIO mode. The port name for this activation attempt was already in use on the other port that belongs to that CHPID. Two ports on the same CHPID cannot have the same port name.
X'3150'	Incorrect port name **Explanation:** An attempt was made to activate an OSA-Express port in QDIO mode. The port name for this activation attempt did not match the port name already assigned to this port by a previous user. All z/OS users of that port must activate with the same port name.
X'32nn'	n/a **Explanation:** Codes starting with X'32' are specific to ATM connection establishment. In particular, they relate to the inability of the IBM Open Systems Adapter to establish a reserved bandwidth connection because of lack of available resources.
X'3201'	Bytes per second exceeded **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of bytes per second that were requested cannot be honored because the IBM Open Systems Adapter's capacity for bytes per second for reserved bandwidth connections would be exceeded.
X'3202'	Receive packets per second exceeded **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of packets per second that were requested in the receive direction (to the IBM Open Systems adapter) cannot be honored because the IBM Open Systems Adapter's capacity for receive packets per second for reserved bandwidth connections would be exceeded.
X'3203'	Transmit packets per second exceeded **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of packets per second that were requested in the transmit direction (from the IBM Open Systems Adapter) cannot be honored because the IBM Open Systems Adapter's capacity for transmit packets per second for reserved bandwidth connections would be exceeded.
X'3204'	No packet buffers available **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of bytes per second that were requested cannot be honored because the IBM Open Systems Adapter's capacity for packet buffers for reserved bandwidth connections would be exceeded.
X'3205'	Bandwidth unavailable **Explanation:** The IBM Open Systems Adapter received a request for a reserved bandwidth circuit. The number of ATM cells per second that were requested cannot be honored because the total number of cells per second would exceed the physical capacity of the ATM link.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'3210'	Network down **Explanation:** The IBM Open Systems Adapter has lost communications to the ATM switch to which it is attached. The OSA lost communication with the attached ATM network, or an attempt was made to activate an XCA while the OSA had lost communication with the network (a missing cable or a switch registration failure, for example.)
X'33nn'	n/a **Explanation:** Codes starting with X'33' are specific to ATM signaling or data transfer. Generally they are the result of either a ULP software or definitional problem in constructing an ATM primitive. Use the specific return code to identify incorrect parameter, termed an information element (IE), to perform diagnostics.
X'330B'	Call does not exist **Explanation:** The Port Control Manager received a primitive associated with a call that no longer or never existed.
X'330D'	Endpoint does not exist **Explanation:** The value of the endpoint reference identifier in the endpoint reference subfield is not currently assigned to a call endpoint.
X'3312'	Service access point not activated **Explanation:** The primitive is incorrect because the SAP is not activated or recognized.
X'3315'	User subfields too large **Explanation:** The subfields specified in the primitive exceed the number of allowable octets.
X'331B'	Subfields not allowed **Explanation:** The subfields contained in the specified primitive are not allowed.
X'331D'	Mandatory subfield missing **Explanation:** A required subfield not present.
X'3323'	Selected channel busy **Explanation:** The specified permanent virtual channel (PVC) is busy or allocated to another call.
X'3324'	Maximum calls exceeded **Explanation:** The call setup request was not executed because the required resource could not be allocated.
X'3329'	Maximum requests exceed **Explanation:** The limit on outstanding primitives was reached.
X'332A'	Call clear indication pending **Explanation:** A call clear indicate has been issued to the user. The user should respond. The call instance is cleared when the call clear response is received from the user.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'332D'	Timeout on call **Explanation:** The call could not be processed within the time constraints of the network.
X'332F'	Lack of resources **Explanation:** The resources requested from the system (for example, memory errors) could not be obtained.
X'3330'	Operating system error **Explanation:** An operating system error was encountered.
X'3331'	Incorrect bearer capability **Explanation:** The length or the parameter information in the bearer capability subfield is incorrect.
X'3332'	Incorrect channel identification **Explanation:** The length or the parameter information in the channel identification subfield is incorrect or the channel not varied online properly by operator.
X'3333'	Incorrect calling party number **Explanation:** The length or the parameter information in the calling party number subfield is incorrect.
X'3334'	Incorrect called party number **Explanation:** The length or the parameter information in the called party number subfield is incorrect.
X'3335'	Incorrect calling party subaddress **Explanation:** The length or the parameter information in the calling party aubaddress subfield is incorrect.
X'3336'	Incorrect called party subaddress **Explanation:** The length or the parameter information in the called party subaddress subfield is incorrect.
X'3337'	Incorrect low-layer compatibility **Explanation:** The length or the parameter information in the low-layer compatibility subfield is incorrect.
X'3338'	Incorrect high-layer compatibility **Explanation:** The length or the parameter information in the high-layer compatibility subfield is incorrect.
X'3339'	Incorrect transit network selection **Explanation:** The length or the parameter information in the transit network selection subfield is incorrect.
X'333A'	Incorrect cause **Explanation:** The length or the parameter information in the cause subfield is incorrect.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'333B'	Incorrect call status **Explanation:** The length or the parameter information in the call status subfield is incorrect.
X'333C'	No cause code specified **Explanation:** The incoming call clearing message from the network did not contain a cause code indicating why the call was being cleared.
X'3340'	Incorrect AAL parameters **Explanation:** The length or parameter values in the AAL parameters subfield is incorrect.
X'3341'	Duplicate AAL parameters **Explanation:** The AAL parameters subfield is specified more than once.
X'3342'	Incorrect endpoint identifier **Explanation:** The length or parameter value in the endpoint reference subfield is incorrect.
X'3343'	Duplicate endpoint reference **Explanation:** The endpoint reference is specified more than once.
X'3344'	Incorrect endpoint state **Explanation:** The length or parameter value in the endpoint status subfield is incorrect.
X'3346'	Incorrect QoS **Explanation:** The length or parameter values in the quality of service subfield is incorrect.
X'3347'	Duplicate QoS **Explanation:** The quality of service subfield is specified more than once.
X'3348'	Incorrect PCI **Explanation:** The length or the parameter value in the permanent connection identifier subfield is incorrect.
X'3349'	Duplicate PCI **Explanation:** The permanent connection identifier subfield is specified more than once.
X'334A'	Incorrect traffic descriptor **Explanation:** The length or the parameter value in the traffic descriptor subfield is incorrect.
X'334B'	Duplicate traffic descriptor **Explanation:** The traffic descriptor subfield is specified more than once.
X'3351'	Duplicate bearer capability **Explanation:** The bearer capability subfield was specified more than one time.
X'3352'	Duplicate channel identification **Explanation:** The channel identification subfield was specified more than one time.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'3353'	Duplicate calling party number **Explanation:** The calling party number subfield was specified more than one time.
X'3354'	Duplicate called party number **Explanation:** The called party number subfield was specified more than one time.
X'3355'	Duplicate calling party subaddress **Explanation:** The calling party subaddress subfield was specified more than one time.
X'3356'	Duplicate called party subaddress **Explanation:** The called party subaddress subfield was specified more than one time.
X'3357'	Too many instances of low-layer information **Explanation:** More instances of low-layer information subfield are present than are allowed.
X'3358'	Duplicate high-layer compatibility **Explanation:** The high-layer compatibility subfield was specified more than one time.
X'3359'	Duplicate Transit network selection **Explanation:** The transit network selection subfield was specified more than one time.
X'335A'	Duplicate cause **Explanation:** The cause subfield was specified more than one time.
X'335B'	Duplicate call status **Explanation:** The call status subfield was specified more than one time.
X'335D'	Duplicate PCI **Explanation:** The permanent connection identifier subfield was specified more than one time.
X'3360'	Subfield of length zero present **Explanation:** One of the subfields in the data information field has a length of zero.
X'3361'	Incorrect calling party number length **Explanation:** In the calling party number subfield, the value that is specified in the SFNumberLength parameter disagrees with the length of the subfield contained in the SFLength parameter.
X'3362'	Incorrect called party number length **Explanation:** In the called party number subfield, the value that is specified in the SFNumberLength parameter disagrees with the length of the subfield contained in the SFLength parameter.
X'3363'	Incorrect calling party subaddress length **Explanation:** In the calling party subaddress subfield, the value that is specified in the SFSubaddrLength parameter disagrees with the length of the subfield contained in the SFLength parameter.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'3364'	Incorrect called party subaddress length **Explanation:** In the called party subaddress subfield, the value that is specified in the SFSubaddrLength parameter disagrees with the length of the subfield contained in the SFLength parameter.
X'3366'	Incorrect call status value **Explanation:** In the call status subfield, the SFCallStatus parameter specifies a value that is incorrect.
X'3367'	Call status subfield missing **Explanation:** The call status subfield information is missing. This is required information for this primitive.
X'336A'	Subfields of the same type are not the same **Explanation:** Two or more subfields of the same type are specified in the data information field; however they are not contiguous.
X'336B'	Entry not unique **Explanation:** The filter registration request is rejected because the call routing information and subfield specifications indicated in the data information field do not make the entry unique. An entry exists in the Port Control Manager incoming call routing table that has the same "must match" information as this request.
X'336C'	First subfield is not primitive specific **Explanation:** The first subfield you specified in the data information field is not the primitive-specific subfield.
X'3371'	Path Control Manager internal error **Explanation:** The Path Control Manager associated with the call detected an internal error.
X'3374'	Permanent connection not defined **Explanation:** The permanent connection that was requested in the call setup request is not defined.
X'3375'	Incorrect ID type in current state **Explanation:** In the current state of the call instance, the identifier type is incorrect.
X'3376'	Call setup confirm for unsuccessful call queued **Explanation:** The Path Control Manager will not process this call clear request because the call that the user requested to be cleared failed.
X'337A'	Prior call control request outstanding **Explanation:** A call control request previously issued by the user has not been confirmed by the Path Control Manager. The user should try the request again after the confirmation is received from the Path Control Manager.
X'3380'	User software error **Explanation:** The user discovered an unexpected software error.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'3393'	Incorrect usage indicator in primitive-specific subfield **Explanation:** The usage indicator provided in the primitive specific subfield on the filter registration request primitive is incorrect. Either the first primitive-specific subfield specified must meet the "must not match" criteria, or the second primitive-specific subfield specified must meet the "must match" criteria.
X'3394'	Incorrect called party address in filter registration request or data transmission flow control state is blocked. **Explanation:** If this error occurs during device activation, the called party number on the filter registration request is incorrect; either it was not supplied, or does not match an address registered to the Path Control Manager. Otherwise a halt data flow request has been sent so data is not flowing.
X'3395'	Connection state incorrect for data transfer **Explanation:** Data cannot be accepted until the data SAP has been processed.
X'3396'	Data transmit flow control blocked for pacing. **Explanation:** The connection over which this data flows is an ATM reserved bandwidth connection. More data has been requested to be sent than has been reserved. The data flow will be blocked for an interval of time to ensure data is not dropped by the ATM network. Data flow will be reopened when the interval of time passes.
X'3397'	Data transmit flow control blocked for remote **Explanation:** The connection over which this data flows is an ATM connection. The IBM Open Systems Adapter has reached a level of congestion and has requested that no more data be sent on this connection until the congestion is relieved. Data flow will be reopened by IBM Open Systems Adapter when the congestion condition has passed.
X'34nn'	n/a **Explanation:** Codes starting with X'34' are specific to the OSA-Express data path. These codes represent errors reported by the OSA-Express adapter relating to the read or write Storage Block Address List Entries (SBALEs).
X'3400'	Error reason unknown **Explanation:** The specific cause of the error cannot be determined.
X'3401'	Invalid buffer contents **Explanation:** The contents of the storage pointed to by the SBALE does not contain a valid OSA-Express header or IP header.
X'3402'	Block crosses 4k boundary **Explanation:** The last byte of the storage represented by the SBALE is not contained in the same 4K storage frame as the first byte.
X'3403'	Invalid fragment type **Explanation:** The SBALE fragment type does not correlate with the fragment type of the previous SBALE.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'3404'	Real address invalid **Explanation:** The SBALE storage address exceeds the size of central storage.
X'40nn'	n/a **Explanation:** Codes starting with X'40' are specific to the VTAM/IBM Open Systems Adapter IDX channel interface.
X'4001'	VTAM/IBM Open Systems Adapter function level mismatch **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed due to function mismatch between VTAM and the IBM Open Systems Adapter; for example, incompatible versions of the two products. Contact system operator to determine cause of the incompatibility.
X'4002'	Incorrect or no header size specified **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange due to MPC specifying an improper header size. Contact VTAM operator to determine cause of the incorrect size.
X'4003'	Incorrect or no block size specified **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange due to MPC specifying an improper I/O buffer size. Contact VTAM operator to determine cause of the incorrect size.
X'4004'	Channel path read write polarity mismatch **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange due to incorrect channel path polarity; for example, read defined as write or write defined as read. The paths were defined incorrectly in either the TRL entry for the device or during IBM Open Systems Adapter configuration. Contact VTAM operator to determine cause of the incorrect size.
X'4005'	VTAM name mismatch **Explanation:** The IBM Open Systems Adapter returned this code indicating request failed during IDX exchange because the same VTAM name was not received over both channel paths. This indicates a condition where two different VTAM instances are configured such that one is trying to use the Read path, the other the Write. Contact VTAM operator to determine correct definition of channel paths.
X'4010'	Channel path pair quiesced **Explanation:** The IBM Open Systems Adapter returned this code indicating that channel paths will be halted due to the failure of some internal IBM Open Systems Adapter process. Contact system operator to determine reason for the IBM Open System Adapter's action.
X'4011'	Incorrect data message size **Explanation:** The IBM Open Systems Adapter returned this code indicating an incorrect message size, normally too large. Channel operation is quiesced and the channel path to the IBM Open Systems Adapter becomes inoperative. Contact VTAM operator or system operator to determine correct maximum message size.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'4080'	Normal termination **Explanation:** MPC uses this code to inform the IBM Open Systems Adapter that normal channel termination is required. It is not normally exposed to the ULP but might appear in the IBM Open Systems Adapter tracing facilities.
X'4081'	VTAM/IBM Open Systems Adapter level mismatch **Explanation:** MPC returned this code indicating initialization request failed due to function mismatch between VTAM and the IBM Open Systems Adapter; for example, incompatible versions of the two products. Contact VTAM operator or system operator to determine cause of the incompatibility.
X'4082'	Channel path read/write polarity error **Explanation:** MPC returned this code indicating initialization request failed due to the IBM Open Systems Adapter specifying an incorrect read or write channel address; the read channel address must be an "even" address and the associated write channel address must be the read address + 1.
X'4083'	Incorrect or no header size specified **Explanation:** MPC returned this code indicating initialization request failed due to the IBM Open Systems Adapter specifying an incorrect header segment size. Contact VTAM operator or system operator to determine cause of the incorrect size.
X'4084'	Incorrect or no buffer size **Explanation:** MPC returned this code indicating initialization request failed due to the IBM Open Systems Adapter specifying an incorrect I/O buffer size. Contact VTAM operator or system operator to determine cause of the I/O buffer size.
X'4085'	Data path failure **Explanation:** MPC returned this code indicating the channel paths to the IBM Open Systems Adapter are now inoperative due to a failure of the data path. Note, this is not a channel failure; it is the failure of a software component that processes data. Failure is normally due to an incorrect data primitive or the occurrence of a VTAM-detected processing error. Contact VTAM operator to perform problem diagnosis.
X'4086'	System failure **Explanation:** MPC returned this code indicating the failure of a process has caused an ABEND within MPC processing components. Failure might be due to an MPC software problem or an underlying system failure. Contact VTAM operator to perform problem diagnosis.
X'4087'	Channel path failure **Explanation:** MPC returned this code indicating the failure of the channel path between itself and the IBM Open Systems Adapter. Failure has been recorded as a long OBR record in the system log. Contact VTAM operator or the system operator to determine cause of failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'4088'	Token failure **Explanation:** MPC uses this code to indicate that the IBM Open Systems Adapter has returned inconsistent token values over the two channel paths. The tokens returned must contain identical bit strings. Contact the system operator to determine cause of inconsistency.
X'4089'	State mismatch **Explanation:** MPC uses this code to indicate that an inconsistency in processing states exists between MPC and the IBM Open Systems Adapter. Contact the VTAM operator to determine cause of inconsistency.
X'408A'	Event Notification Facility offline signal **Explanation:** MPC uses this code to indicate that an Event Notification Signal (ENF) has been received indicating the channel paths have been varied offline. Contact the system operator to determine reason the paths were put offline.
X'408B'	No storage for I/O buffer **Explanation:** MPC uses this code to indicate that storage was not available for it to build the required channel I/O buffers for the data and header segments. System storage might be constrained due to competing requests for storage. Contact the VTAM operator to determine VTAM's current storage usage and the system operator to determine cause of storage scarcity.
X'408C'	Incorrect IBM Open Systems Adapter name **Explanation:** The name used to activate the IBM Open Systems Adapter does not match the defined value. Check your definitions.
X'408D'	Channel control failure **Explanation:** MPC uses this code to indicate a failure in its channel control (CC) component. The failure might have been caused by a software failure in the CC component or an underlying system failure. Contact the VTAM operator to determine failure cause. If a system failure, notify the system operator.
X'408E'	Signaling plane failure **Explanation:** MPC uses this code to indicate a failure in the signaling plane. Contact the VTAM operator to determine failure cause. If a system failure, notify the system operator.
X'50nn'	Shared Memory Communications over Remote Direct Memory Access (SMC-R) failures **Explanation:** Codes starting with X'50' are specific to SMC-R operation failures. Use the specific return code to help identify the problem.
X'5001'	Peripheral Component Interconnect Express (PCIe) function ID (PFID) is not valid **Explanation:** The PFID value that is specified on the activation attempt contained characters that are not valid or that did not match the PFID of any active "RoCE Express" interface.
X'5002'	The buffer size of the outbound buffer is not valid **Explanation:** The buffer size that is specified for a buffer to be used for outbound RDMA operations was too large or represented only a partial buffer.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'5003'	The buffer size of the inbound buffer is not valid **Explanation:** The buffer size that is specified for a buffer to be used for inbound RDMA operations was too large or represented only a partial buffer.
X'5004'	The outbound RDMA buffer could not be registered **Explanation:** The buffer to be used for outbound RDMA operations could not be registered with the "RoCE Express" interface because the buffer descriptor on the primitive request did not contain the correct information.
X'5005'	The inbound RDMA buffer could not be registered **Explanation:** The buffer to be used for inbound RDMA operations could not be registered with the "RoCE Express" interface because the buffer descriptor on the primitive request did not contain the correct information.
X'5006'	Incorrect primitive **Explanation:** The value that is specified in the primitive code parameter of the control information field is not correct.
X'5008'	Maximum users exceeded **Explanation:** The activation request attempted for this adapter exceeds the allowable number of adapter users.
X'5009'	Internal state error **Explanation:** The primitive request is received in an unexpected adapter state.
X'500A'	Virtual LAN (VLAN) identifier is not valid **Explanation:** The value that is specified for the VLAN identifier on the activation request exceeds the maximum value allowed.
X'500B'	Incorrect SMC-R link activation message **Explanation:** The SMC-R link activation message that is received from the SMC-R peer contained no data or the data specified was incorrect.
X'500C'	Queue pair (QP) activation timed out **Explanation:** The attempt to activate a QP as part of SMC-R link establishment did not complete within an acceptable amount of time.
X'500D'	Internal abend **Explanation:** VTAM returns this code to indicate that the failure of a process caused an abnormal end of task (abend) within SMC-R processing components. A software problem or an underlying system failure might be the cause. Contact the VTAM operator to perform problem diagnosis.
X'500E'	Unable to schedule TCP/IP during interrupt processing **Explanation:** During a normal interrupt completion event, VTAM was unable to schedule the TCP/IP stack to process inbound data.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'500F'	SMC-R VLAN disabled **Explanation:** The TCP/IP stack requested VTAM to disable a specific VLAN. As a result, all QPs that are associated with this VLAN are stopped.
X'5010'	RDMA over Converged Ethernet (RoCE) token is not valid **Explanation:** The value that is specified for the RoCE token on the primitive was 0 or did not match any currently assigned tokens.
X'5011'	VLAN token is not valid **Explanation:** The value that is specified for the VLAN token on the primitive did not match any currently assigned tokens.
X'5012'	QP token is not valid **Explanation:** The value that is specified for the QP token on the primitive was 0 or did not match any currently assigned tokens.
X'5013'	SMC-R link activation failure **Explanation:** VTAM could not successfully send the appropriate link activation message to the peer, preventing the SMC-R link from being activated.
X'5014'	Internal stall error detected **Explanation:** The SMC-R components determined that no outbound RDMA operations completed within an acceptable period. INOP processing is triggered for the "RoCE Express" interface.
X'5015'	Internal poll error detected **Explanation:** An attempt by the SMC-R components to poll the "RoCE Express" interface for information about outbound RDMA operations failed unexpectedly. INOP processing is triggered for the "RoCE Express" interface.
X'5016'	Outbound RDMA operations cannot be queued **Explanation:** The SMC-R components determined that pending outbound RDMA operations must be queued because of "RoCE Express" interface conditions, but this primitive indicated that it cannot be queued. The primitive is not queued.
X'5017'	Internal failure during "RoCE Express" interface cleanup **Explanation:** The SMC-R components could not perform a final poll of the "RoCE Express" interface for information about outbound RDMA operations before deactivating the "RoCE Express" interface.
X'5018'	Could not schedule stack to process RDMA data **Explanation:** The SMC-R components could not schedule a TCP/IP process to receive RDMA data.
X'5019'	Queue pair (QP) activation timeout threshold exceeded **Explanation:** The SMC-R components detected repeated failures when activating a QP for an individual "RoCE Express" interface. INOP processing is triggered for the interface.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'501A'	Invalid SMC Version **Explanation:** The primitive request is received with an invalid SMC version.
X'5020'	A CSDUMP was taken with a defined RNICTRLE that matched this "RoCE Express" interface. **Explanation:** A CSDUMP operation, with the RNICTRLE operand specified, requested that diagnostic data be gathered for a "RoCE Express" interface. The process of collecting this data rendered the "RoCE Express" feature inoperative for all users.
X'5021'	"RoCE Express" interface deactivated because a hardware diagnostic dump was taken **Explanation:** A "RoCE Express" interface was deactivated for one the following reasons: • An INOPDUMP was taken for the "RoCE Express" interface. • A CSDUMP was taken and a diagnostic dump was requested by using the RNICTRLE parameter. **Note:** The gathering of diagnostic data causes an inoperative condition for all users.
X'5022'	"RoCE Express" interface deactivated because "RoCE Express" internal error was detected **Explanation:** A "RoCE Express" interface was deactivated because the interface reported an internal error. To recover from the internal error, VTAM resets the "RoCE Express" interface and the "RoCE Express" interface is temporarily unavailable for all users.
X'51nn'	"RoCE Express" device driver failure **Explanation:** In response to specific RoCE verb invocation failures, the "RoCE Express" device driver sets the codes that start with X'51'. These codes are internally generated software codes that identify failures to communicate correctly with PCIe services or with the hardware. • For PCIe service failures, the "RoCE Express" device driver issues message IST2390I or IST2391I to report these failures. In these cases, the *nn* portion of the error code represents the return code that was recorded for the specific PCIe service failure. • For all other failures, the *nn* portion of the error is an internally generated value to uniquely identify the failure.
X'5113'	PFID is not defined **Explanation:** The "RoCE Express" device driver attempted to activate a "RoCE Express" interface, but the PFIDs value is not defined for this LPAR. The "RoCE Express" device driver issues message IST2392I to report this failure.
X'5115'	PFID is not online **Explanation:** The "RoCE Express" device driver attempted to activate a "RoCE Express" interface, but the PFID value is not configured online. The "RoCE Express" device driver issues message IST2393I to report this failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'5116'	Command operation timeout **Explanation:** One of the following cases happened: • The 10 GbE RoCE Express device driver issued a Host channel adapter (HCA) configuration register (HCR) command to the RoCE hardware, but the hardware did not complete the operation within the internally specified timeout threshold. • The RoCE Express2 device driver issued a HCA command queue (HCQ) command to the RoCE hardware, but the hardware did not complete the operation within the internally specified timeout threshold. The "RoCE Express" device driver initiates INOP processing to recover from the error.
X'5117'	PCIe load operation failure **Explanation:** During the processing of an HCR operation for a 10 GbE RoCE Express feature or an HCQ operation for a RoCE Express2 feature, the "RoCE Express" device driver received an error in response to a PCIe store operation. The "RoCE Express" device driver might initiate INOP processing to recover from this error.
X'5118'	PCIe store operation failure **Explanation:** During the processing of an HCR operation for a 10 GbE RoCE Express feature or an HCQ operation for a RoCE Express2 feature, the "RoCE Express" device driver received an error in response to a PCIe store operation. The "RoCE Express" device driver might initiate INOP processing to recover from this error.
X'5121'	Command operation failure **Explanation:** One of the following cases happened: • The 10 GbE RoCE Express device driver issued an HCR command to the RoCE hardware, but the hardware rejected the operation with a specific status code. • The RoCE Express2 device driver issued an HCQ command to the RoCE hardware, but the hardware rejected the operation with a specific status code. The specific operation failed.
X'5131'	PCIe connect service call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe connect service call (IQP4CON) during the activation of a "RoCE Express" interface. The "RoCE Express" device driver issues message IST2391I to report this failure.
X'5132'	PCIe open service call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe open service call (IQP4OPN) during the activation of a "RoCE Express" interface. The "RoCE Express" device driver issues message IST2391I to report this failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5138'	PCIe deregister service call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe deregister service call (IQP4DMR) in one of the following situations: • When a "RoCE Express" interface is deactivated. • When the TCP/IP stack contracts a storage pool and attempts to deregister specific memory regions. The "RoCE Express" device driver issues message IST2391I to report this failure.
X'513B'	Software reset failure **Explanation:** While the "RoCE Express" device was initialized, the "RoCE Express" device driver received an error during a software reset of the "RoCE Express" feature. This call is issued during the activation of a "RoCE Express" interface. The "RoCE Express" interface does not activate.
X'5140'	PCIe close service call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe close service call (IQP4CLO) during the deactivation of a "RoCE Express" interface. The "RoCE Express" device driver issues message IST2391I to report this failure.
X'5141'	PCIe deallocation service call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe deallocation service call (IQP4DEA) during the deactivation of a "RoCE Express" interface. The "RoCE Express" device driver issues message IST2391I to report this failure.
X'5142'	PCIe address space not available **Explanation:** The "RoCE Express" device driver detected the PCIe address has not been initialized. The "RoCE Express" device driver requires PCIe service calls to activate a "RoCE Express" interface. The "RoCE Express" device driver fails the activation request.
X'5144'	PCIe allocation service call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe allocation service call (IQP4ALL) during the activation of a "RoCE Express" interface. The "RoCE Express" device driver issues message IST2391I to report this failure.
X'514A'	No physical network ID detected **Explanation:** The "RoCE Express" device driver issued a PCIe service call (IQP4GDI) to learn information about a "RoCE Express" interface. The "RoCE Express" device driver detected that no physical network ID (PNetID) was configured for this PFID. A "RoCE Express" interface without a configured PNetID cannot be used for SMC-R communications. The "RoCE Express" device driver issues message IST2391I to report this failure.
X'5150'	PCIe service processor call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe service processor call (IQP4SPC) to collect diagnostic hardware information during the INOPDUMP or the CSDUMP processing. The "RoCE Express" device driver issues message IST2391I to report this failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5151'	Incorrect operating environment detected for the IBM 10 GbE RoCE Express feature **Explanation:** A 10 GbE RoCE Express feature was configured in the hardware configuration definition (HCD) to run in a dedicated RoCE environment, but z/OS Communications Server expected the feature to run in a shared RoCE environment. Another possible situation is that a 10 GbE RoCE Express feature was configured to run in a shared RoCE environment, but z/OS Communications Server expected the feature to run in a dedicated RoCE environment. The first 10 GbE RoCE Express feature to be activated determines the operating environment for all subsequent features.
X'515B'	PCIe get device information service call failure **Explanation:** The "RoCE Express" device driver received an error in response to a PCIe get device information service call (IQP4GDI) during the activation of a "RoCE Express" interface. The "RoCE Express" device driver issues message IST2391I to report this failure.
X'515D'	Unexpected error occurred on the Ethernet RQ or SQ **Explanation:** The "RoCE Express" device driver received an error for either the Ethernet Receive Queue (RQ) or Send Queue (SQ). The "RoCE Express" device driver initiates INOP processing to recover from this error.
X'52nn'	TCP/IP SMC-R component failures during SMC-R processing **Explanation:** Codes that start with X'52' are specific to failures that are encountered within the TCP/IP SMC-R components during SMC-R processing. These errors cause the TCP connection to not use the SMC-R protocols.
X'5226'	SMC-Rv2 link failure, link activation failed **Explanation:** No route found to the SMC-Rv2 IP address for the remote peer. As a result, an SMC-Rv2 link cannot be established between the two peers.
X'52E0'	SMC-R link failure, no failover processing **Explanation:** The TCP/IP stack detected that an SMC-R link failed and no alternative SMC-R link was available.
X'52E1'	SMC-R link failure, local and remote partners are out of synch **Explanation:** The TCP/IP stack attempted to establish an initial SMC-R link to the remote partner, but the partner detects that an SMC-R link exists between the two endpoints.
X'52F0'	SMC-R link failure, failover processing **Explanation:** The TCP/IP stack detected that an SMC-R link failed. The TCP/IP stack switched the TCP connections that were using the failing SMC-R link to an alternative link within the SMC-R link group.
X'52F1'	SMC-R link failure, loss of path detected **Explanation:** The TCP/IP stack was notified that the RDMA path for an SMC-R link failed.
X'52F2'	SMC-R link failure, protocol violation **Explanation:** The TCP/IP stack detected that an SMC-R link failed because of a violation of the Link Layer Control (LLC) protocol that is used to manage the link.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'52F3'	SMC-R link failure, RDMA write operation failed **Explanation:** The TCP/IP stack detected that an attempt to write RDMA data over an SMC-R link failed.
X'52F4'	SMC-R link failure, remote buffer confirmation time out **Explanation:** The TCP/IP stack detected that the remote partner did not confirm that an SMC-R link used a remote buffer. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group. **Tip:** You might see this error if SMC-R is operating in networks with persistent congestion and packet loss (i.e. switches, routers) which leads to the time-out condition.
X'52F5'	SMC-R link failure, delete buffer time out **Explanation:** The TCP/IP stack detected that the remote partner did not acknowledge that a buffer was no longer available for an SMC-R link to use. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group. **Tip:** You might see this error if SMC-R is operating in networks with persistent congestion and packet loss (i.e. switches, routers) which leads to the time-out condition.
X'52F6'	SMC-R link failure, link deletion time out **Explanation:** The TCP/IP stack attempted to delete an SMC-R link from a link group, but the remote partner did not acknowledge the request. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group. **Tip:** You might see this error if SMC-R is operating in networks with persistent congestion and packet loss (i.e. switches, routers) which leads to the time-out condition.
X'52F7'	SMC-R link failure, link test time out **Explanation:** The TCP/IP stack tested the status of an SMC-R link, but the remote partner did not respond to the test request. The SMC-R link was assumed to be inactive and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group. **Tip:** You might see this error if SMC-R is operating in networks with persistent congestion and packet loss (i.e. switches, routers) which leads to the time-out condition.
X'52F8'	SMC-R link failure, link addition time out **Explanation:** The TCP/IP stack attempted to add an SMC-R link to a link group, but the remote partner did not acknowledge the request. The link was stopped and, if possible, the TCP connections that were using the stopped link were switched to an alternative link in the link group. **Tip:** You might see this error if SMC-R is operating in networks with persistent congestion and packet loss (i.e. switches, routers) which leads to the time-out condition.
X'52FA'	SMC-R link failure due to TCP connection termination **Explanation:** The initial TCP connection that caused the creation of a new SMC-R link between two peers has stopped. As a result, the new SMC-R link being established is also stopped. The remote peer might report another DLC status code in this SMC-R link failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'53nn'	TCP/IP stack failures during SMC-R processing **Explanation:** Codes that start with X'53' are specific to failures that the TCP/IP stack encountered during SMC-R processing. These errors cause the TCP connection to not use the SMC-R protocols.
X'54nn'	"RoCE Express" interrupt handler errors **Explanation:** Codes that start with X'54' are specific to failures that the "RoCE Express" interrupt handlers encountered. The "RoCE Express" interrupt handlers are associated with a "RoCE Express" interface. These failures cause VTAM to initiate INOP processing of the "RoCE Express" interface. For these failures, the *nn* portion of the error code represents the 1-byte event code that the "RoCE Express" interface generates.
X'5409'	Port state event **Explanation:** The disabled interrupt exit was driven by PCIe services to notify the "RoCE Express" device driver that the state of the "RoCE Express" port is inactive. The "RoCE Express" device driver initiates INOP processing for all TCP/IP stacks with active connections to this "RoCE Express" interface.
X'54F0'	Allocation error exit **Explanation:** PCIe services drove the "RoCE Express" allocation error exit to inform the "RoCE Express" device driver of a PCIe error event. The "RoCE Express" device driver initiates INOP processing for all TCP/IP stacks with active connections to this "RoCE Express" interface.
X'54F1'	Open error exit **Explanation:** PCIe services drove the "RoCE Express" open error exit to inform the TCP/IP stack that the PFID was deallocated. This code can be issued for one of the following reasons: • The "RoCE Express" device driver detected an error that caused the Force Close processing to take down the "RoCE Express" interface. • PCIe services detected a condition that required the deallocation of a PFID that VTAM allocated. In either case, "RoCE Express" device driver initiates INOP processing for the reported TCP/IP stack.
X'54F2'	Event Queue (EQ) Doorbell error **Explanation:** The "RoCE Express" device driver did a PCIe store operation to notify the "RoCE Express" interface that the driver finished processing event queue elements. The store operation completed with an error. The "RoCE Express" device driver initiates INOP processing for all TCP/IP stacks with active connections to the "RoCE Express" interface.
X'55nn'	SMC-R link failure, RDMA write operation did not complete successfully **Explanation:** Codes that start with X'55' are specific to RDMA write-completion failures that are reported to the TCP/IP stack. These failures cause the TCP/IP stack to stop the SMC-R link that is associated with the failed RDMA write operation. If possible, the TCP/IP stack switches the TCP connections that are using the link to another link within the SMC-R link group. For these failures, the *nn* portion of the error code represents the 1-byte event code that the "RoCE Express" interface generates to report the write completion failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5515'	SMC-R link failure, RDMA Write operation failure: retries exhausted **Explanation:** An RDMA Write or Send operation failed transmission and the result is reported to the TCP/IP stack. This type of failure causes the TCP/IP stack to stop the SMC-R link that is associated with the failed operation. If possible, the TCP/IP stack switches the TCP connections that are using the link to another link within the SMC-R link group. For this specific failure, the "RoCE Express" adapter transmitted packets to the partner SMC-R link, but failed to receive an acknowledgment from the peer "RoCE Express" adapter. The operation is retried for a predetermined number of retries, but the data was not acknowledged. **Tip:** You might see this error if SMC-R is operating in networks with persistent congestion and packet loss (i.e. switches, routers) which leads to the transmission failure.
X'56nn'	Shared Memory Communications - Direct Memory Access (SMC-D) failures **Explanation:** Codes that begin with X'56' are specific to SMC-D operation failures. Use the specific return code to identify the problem.
X'5601'	The buffer size of the outbound buffer is not valid **Explanation:** The size that was specified for a buffer to be used for outbound internal shared memory (ISM) operations was too large or represented only a partial buffer.
X'5602'	The ISM buffer could not be registered **Explanation:** The buffer to be used for ISM operations could not be registered because the buffer descriptor on the primitive request did not contain necessary information.
X'5603'	Incorrect primitive **Explanation:** The value that was specified in the primitive code parameter of the control information field is not correct.
X'5604'	Internal state error **Explanation:** The primitive request was received in an unexpected device state.
X'5605'	Virtual LAN (VLAN) identifier is not valid **Explanation:** The value that was specified for the VLAN identifier on the activation request exceeds the maximum allowed value.
X'5606'	Internal abend **Explanation:** VTAM returns this code to indicate that the failure of a process has caused an abnormal end of task (abend) within SMC-D processing components. The failure might be caused by a software problem or might be an underlying system failure. Contact the VTAM operator to diagnose the problem.
X'5607'	Internal failure during INOP processing **Explanation:** VTAM could not notify a user of the ISM device while processing an INOP condition.
X'5608'	Internal shared memory (ISM) token is not valid **Explanation:** The value that was specified for the ISM token on the primitive was 0 or did not match any currently assigned tokens.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'5609'	VLAN token is not valid **Explanation:** The value that was specified for the VLAN token on the primitive was 0, exceeded the maximum allowed value, or did not match any currently assigned tokens.
X'560A'	SMC-D link token is not valid **Explanation:** The value that was specified for the SMC-D link on the primitive was 0 or did not match any currently assigned tokens.
X'560B'	No more buffers can be registered with the ISM device **Explanation:** The attempt to register a buffer for ISM operations failed because no index bits were available to represent the buffer. A maximum of 1920 buffers can be registered with an individual ISM device.
X'57nn'	Internal shared memory (ISM) function failure **Explanation:** Codes that begin with X'57' are specific to ISM verb invocation failures. For these failures, the 'nn' portion of the error code represents the return code that the ISM device generated in response to an ISM verb invocation.
X'5701'	PCIe Search (IQP4SRC) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe search service call (IQP4SRC) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5702'	No ISM PFIDs are defined for physical network ID (PNetID) **Explanation:** The ISM device driver issued a PCIe search service call (IQP4SRC) to detect all defined ISM PFIDs for the PNetID that is associated with the QDIO or iQDIO interface that the TCP/IP stack activated. The ISM device driver detected that no ISM PFIDs were defined for this specific PNetID. Therefore, the TCP/IP stack cannot use SMC-D communications for this PNetID. The ISM device driver issues message IST2422I to report this failure.
X'5703'	No ISM PFIDs are available for PNetID **Explanation:** The ISM device driver issued a PCIe search service call (IQP4SRC) to detect all defined ISM PFIDs for the PNetID that is associated with the QDIO or iQDIO interface that the TCP/IP stack activated. The ISM device driver detected that ISM PFIDs are defined for this PNetID, but none of the PFIDs are currently available. Therefore, the TCP/IP stack cannot use SMC-D communications for this PNetID. The ISM device driver issues message IST2423I to report this failure.
X'5704'	PCIe Get PFID Information (IQP4GPI) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Get PFID Information service call (IQP4GPI) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5705'	PCIe Get Device Information (IQP4GDI) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Get Device Information service call (IQP4GDI) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'5706'	PCIe Register Memory Region (IQP4RMR) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Register Memory Region service call (IQP4RMR). The ISM device driver issues message IST2391I to report this failure.
X'5707'	HVCommon storage allocation failure **Explanation:** The ISM device driver received an error in response to an IARV64 macro invocation to obtain high virtual common storage during the activation of an ISM interface.
X'5708'	Partner not reachable via SMC-D **Explanation:** The partner host supports SMC-D, but the partner is not reachable via SMC-D. For example, the partner host might be located on a different CEC, the partner host might not have SMC-D enabled for the same PNetID, or the defined VLANs for SMC-D are not consistent across the hosts.
X'5713'	PFID is not defined **Explanation:** The ISM device driver attempted to activate an ISM interface, but the PFID value that is detected through the PCIe search (IQP4SRC) service is not defined for this LPAR. The ISM device driver issues message IST2392I to report this failure.
X'5715'	PFID is not online **Explanation:** The ISM device driver attempted to activate an ISM interface, but the PFID value is not configured online. The ISM device driver issues message IST2393I to report this failure.
X'5717'	PCIe load operation failure **Explanation:** During the processing of an ICR operation, the ISM device driver received an error in response to a PCIe load operation. The ISM device driver might initiate INOP processing to recover from this error.
X'5718'	PCIe store operation failure **Explanation:** During the processing of an ICR operation, the ISM device driver received an error in response to a PCIe store operation. The ISM device driver might initiate INOP processing to recover from this error.
X'5721'	ICR command operation failure **Explanation:** The ISM device driver issued an ICR command to the ISM firmware, but the firmware rejected the operation with a specific command result. The specific ICR operation failed.
X'5731'	PCIe Connect (IQP4CON) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe connect service call (IQP4CON) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5732'	PCIe Open (IQP4OPN) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe open service call (IQP4OPN) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)

Hexadecimal Code	Meaning
X'5738'	PCIe Deregister Memory Region (IQP4DMR) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe deregister service call (IQP4DMR) in one of the following situations: • When an ISM interface is deactivated. • When the TCP/IP stack contracts a direct memory buffer (DMB) storage pool and attempts to deregister specific memory regions. The ISM device driver issues message IST2391I to report this failure.
X'5740'	PCIe Close (IQP4CLO) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Close service call (IQP4CLO) during the deactivation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5741'	PCIe Deallocation (IQP4DEA) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe deallocation service call (IQP4DEA) during the deactivation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5742'	PCIe address space not available **Explanation:** The ISM device driver detected the PCIe address has not been initialized. The ISM device driver requires PCIe service calls to activate an ISM interface. The ISM device driver fails the ISM interface activation request.
X'5744'	PCIe Allocation (IQP4ALL) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe allocation service call (IQP4ALL) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.
X'5747'	Maximum number of registered direct memory buffers (DMBs) is reached **Explanation:** The TCP/IP stack attempted to expand the DMB storage pool by registering additional memory regions. The ISM device driver detected that it reached the maximum number of DMBs, which is allowed to register with ISM firmware. The DMB storage expansion request is failed.
X'5749'	Duplicate ICR operation **Explanation:** During the processing of an ICR operation, the ISM device driver received an error from the ISM firmware that the requested operation is a duplicate operation. The requested ISM operation was not performed.
X'574A'	Required hardware is not available **Explanation:** The ISM device driver detected that ISM processing cannot be performed because the necessary hardware is not available. The ISM device driver issues message IST2420I to report this failure.
X'574B'	PCIe Query System Characteristics (IQP4QSC) service call failure **Explanation:** The ISM device driver received an error in response to a PCIe Query System Characteristics service call (IQP4QSC) during the activation of an ISM interface. The ISM device driver issues message IST2391I to report this failure.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
X'58nn'	TCP/IP SMC-D componentry failures during SMC-D processing **Explanation:** Codes that begin with X'58' are specific to failures that are encountered within the TCP/IP SMC-D components during SMC-D processing. These errors cause the TCP connection to not use the SMC-D protocols.
X'59nn'	Internal shared memory (ISM) device interrupt handler errors **Explanation:** Codes that begin with X'59' are specific to failures that are encountered by the Disabled Interrupt Handler that is associated with an ISM device. These failures cause VTAM to initiate INOP processing of the ISM device. For these failures, the 'nn' portion of the error code represents the 1-byte event code that the ISM device generates.
x'5Ann'	z/OS Container Extensions Direct Network Interface (DNI) failures. **Explanation:** Codes starting with X'5A' are specific to z/OS Container Extensions DNI operation failures. Use the specific return code to help identify the problem.
x'5A01'	Function code not supported. **Explanation:** The requested DNI function code is not supported.
x'5A02'	Service type not supported. **Explanation:** The requested DNI service type function code is not supported.
x'5A03'	Provider ID error. **Explanation:** The provider ID passed on a DNI send or DNI disconnect operation is either incorrect or is no longer valid.
x'5A04'	State error. **Explanation:** An unexpected state was encountered while processing the current DNI request.
x'5A05'	Buffer list entry length error. **Explanation:** A DNI send request was found to contain a buffer list entry which contained a zero length.
x'5A06'	Send length mismatch. **Explanation:** A DNI send request was found to have the total length of data in the buffer list chain field not to match the sum of all the buffer list entries lengths.
x'5A07'	Buffer list count exceeds maximum. **Explanation:** A DNI send request exceeded the maximum number of buffer list entries.
x'5A08'	Maximum packet size exceeded. **Explanation:** The DNI send request specified a packet which exceeds the MTU size of the EZAZCX interface.
x'5A09'	Invalid version of DNI parameter list. **Explanation:** The DNI request specified an unsupported version of the DNI parameter list.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
x'5A0A'	DNI user authorization failure 1. **Explanation:** An attempt was made to use z/OS Container Extensions DNI services, but one of the required authorization checks was not met.
x'5A0B'	DNI user authorization failure 2. **Explanation:** An attempt was made to use z/OS Container Extensions DNI services, but one of the required authorization checks was not met.
x'5A0C'	DNI connect failure. **Explanation:** The DNI connect request was issued in SRB mode. The connect call requires TCB mode.
x'5A0D'	DNI service not available. **Explanation:** While processing a DNI connect request, a problem occurred while: • Trying to locate the TCP/IP stack configured to support the dynamic VIPA for z/OS Container Extensions. • The dynamic VIPA was being activated in the target stack on behalf of the z/OS Container Extensions user.
x'5A0E'	TCP/IP stack not available. **Explanation:** While processing a DNI connect request, the TCP/IP stack configured to support the dynamic VIPA for z/OS Container Extensions was not found. A DNI user could also have its signal exit driven with a disconnect indicate containing this reason when the target TCP/IP stack's EZAZCX or EZ6ZCX interface becomes inactive.
x'5A0F'	Storage not available. **Explanation:** While processing a DNI request, a storage not available condition was encountered.
x'5A10'	IUTIL macro failure. **Explanation:** The DNI device driver received an IUTIL operation failure while trying to service a DNI request.
x'5A11'	Protocol version not supported. **Explanation:** A DNI request was received which specified an unsupported protocol version.
x'5A12'	Internal WAIT error. **Explanation:** While processing a DNI request, an unexpected error occurred while processing a WAIT operation.
x'5A13'	OMVS not available. **Explanation:** While processing a DNI connect request, an error occurred because OMVS services is not available.
x'5A14'	Internal Error - Out of indices. **Explanation:** While processing a DNI connect request, the DNI device driver determined there were no available indices to assign the new DNI user.

Table 11. Bytes 2 and 3 (completion code) of the DLC status code (continued)	
Hexadecimal Code	**Meaning**
x'5A15'	Required information missing. **Explanation:** While processing a DNI request, required information was missing from the DNI parameter list.
x'5A16'	Unexpected IUTIL signal received. **Explanation:** An unexpected IUTIL signal was received from VTAM for the current FSM state of the DNI user.
x'5A17'	Bad user data. **Explanation:** While setting up a DNI connection, the DNI component received the expected IUTIL signal however the user data within that signal contained invalid information.
x'5A18'	Deactivate SAP IUTIL signal received. **Explanation:** The DNI component received an unexpected but valid Deactivate SAP Indicate IUTIL signal from VTAM. The z/OS Container Extensions connection is no longer usable. As a result, the DNI component has driven the signal exit of the DNI user with a disconnect indicate.
x'5A19'	Internal abend. **Explanation:** The DNI component returns this code to indicate that the failure of a process caused an abnormal end of task (abend) within DNI processing components. A software problem or an underlying system failure might be the cause.
x'5A1A'	IUTILZ error occurred. **Explanation:** The DNI component returns this code to indicate that an IUTILZ macro failed on the datapath.
x'5A1B'	Invalid MTU specified in DNI parameter list. **Explanation:** The DNI request specified an invalid MTU value. The value must be within the range of 1280 - 65535.

Chapter 4. CSM monitor IDs

This chapter contains the CSM monitor IDs.

Hexadecimal value	Monitor ID description	Symbol	Notes
X'00' – X'1F' CSM Monitor IDs			
X'00'	CSM Owned buffer	CSM_OWN	
X'01'	CSM Get buffer	CSM_GETBUF	
X'02'	CSM Assign buffer	CSM_ASGNBUF	
X'03'	CSM Free buffer	CSM_FREEBUF	
X'20' – X'2F' DLC Monitor IDs			
X'20'	DLC Write Operation	IUT_Req	1,3
X'21'	DLC Read Operation	IUT_ReadBfr	2,3
X'22'	DLC Read Completed (Inbound ULP)	DLC Read Completed (Inbound ULP) IUT_Ind	
X'23'	DLC Cached	DLC Cached IUT_Cached	
X'24'	DLC Cached IQDR (iQDIO)	IUT_Cached_IQDR	
X'25'	IUTILZ VTAM	IUT_zCX_VTAM	
X'26'	zCX IUTILZ Inbound Stack	IUT_zCX_Stack	
X'27'	zCX IUTILZ Inbound Server	IUT_zCX_Server	
X'30' – X'8F' VTAM Unique Monitor IDs			
X'30'	RTP Outbound Start	RTP_OUT_START	
X'31'	RTP Outbound Done	RTP_OUT_DONE	
X'32'	RTP Out Garbage	RTP_OUT_GARBAGE	
X'33'	RTP In Start	RTP_IN_START	
X'34'	RTP In Continue	RTP_IN_CONTINUE	
X'35'	RTP In Done	RTP_IN_DONE	
X'38'	TSC	TSC	
X'39'	TSC BF Pacing	TSC_BFPacing	
X'3A'	TSC XCF	TSC_XCF	
X'3B'	CFS SWSA	CFS_SWSA	4
X'3C'	CFS Sysplex Ports	CFS_Sysplexports	4
X'3D'	PS buffer	PS	
X'3E'	TSIP buffer	TSIP	
X'3F'	RCM buffer	RCM	
X'40'	TSCMO buffer	TSCMO	

© Copyright IBM Corp. 2000, 2021

Hexadecimal value	Monitor ID description	Symbol	Notes
X'41'	TSCSH buffer	TSCSH	
X'42'	TSCSX buffer	TSCSX	
X'43'	RPCRN buffer	RPCRN	
x'44'	Allocated by GETBLK	O64GB	
x'45'	Cached by zCX DNI	DNI_Cached	
x'46'	DNI outbound	DNI_Outbound	
x'47'	DNI inbound	DNI_Inbound	
X'50'	SMC-R Read Completion container, available	SMCR_RC_Cached	
X'51'	SMC-R Read Completion container, completed	SMCR_RC_Ind	
X'52'	SMC-R Write Completion container, available	SMCR_WC_Cached	
X'53'	SMC-R Write Completion container, completed	SMCR_WC_Ind	
X'54'	SMC-R Write Completion container, queued	SMCR_WC_PendInd	
X'90' – X'FF' TCP/IP Monitor IDs			
X'90' – X'97' IF Layer Monitor IDs			
X'90'	IF Inbound	ifInbound	5
X'91'	IF Outbound	ifOutbound	
X'92'	IF Blocking/Packing	ifBlockPack	
X'93'	F User Free Processing	IfUserfree	
X'94'	IF Control Packet	ifControlPacket	
X'95'	IF Termination	ifTermination	
X'96'	IF HiperSockets Accelerator Inbound	hsAccInbound	
X'97'	IF HiperSockets Accelerator Outbound	hsAccOutbound	
X'98' – X'9F' IP Layer Monitor IDs			
X'98'	IP Inbound	ipInbound	
X'99'	IP Outbound	ipOutbound	
X'9A'	Firewall Inbound	fwInbound	
X'9B'	Firewall Outbound	fwOutbound	
X'9C'	ICMP	icmp	
X'9D'	IGMP	igmp	
X'9E'	IP Queue	ipQueue	
X'A0' – X'AF' Transport Layer Monitor IDs			

Hexadecimal value	Monitor ID description	Symbol	Notes
X'A0'	Raw Inbound	rawInbound	
X'A1'	Raw Outbound	rawOutbound	
X'A4'	TCP Inbound	tcpInbound	
X'A5'	TCP Outbound	tcpOutbound	
X'A8'	UDP Inbound	udpInbound	5
X'A9'	UDP Outbound	udpOutbound	
X'AC'	EE Inbound	eeInbound	
X'AD'	EE Outbound	eeOutbound	
X'B0' – X'FF' TCP/IP Misc Monitor IDs			
X'B0'	Streams	streams	
X'B1'	Storage	itStorage	
X'B2'	XCF	xcf	
X'B3'	PFS	pfs	
X'B4'	AFPA	afpa	
X'B5'	Firewall IPSec	fwipsec	
X'C0'	Application FTP	applFtp	
X'C1'	Application SNALINK	applSnalink	
X'C2'	Application X25	applX25	
X'C3®'	Application IPSEC	applIpsec	

Note:

1. For monitor ID X'20', the user data field will provide the EBCDIC subchannel write device unit address associated with this device. Users should monitor this device for capacity issues.
2. For monitor ID X'21', the user field will provide the EBCDIC subchannel read device unit address associated with this device. Some devices can configure how much read storage is used (for example, QDIO devices).
3. Storage associated with DLC monitor IDs can be influenced by both SNA and TCP/IP workloads.
4. This monitor ID is associated with a common service provided by z/OS Communications Server, but is primarily associated with TCP/IP functions and application workloads.
5. For TCP/IP inbound processing, a single buffer is used for many datagrams. The message triples are used to keep track of the datagrams. These message triples are used with DUPB operand.

Chapter 5. VTAM status codes

This chapter includes the following resource and session status information:

- "Resource status codes and modifiers" on page 265
  - "Resource state code categories" on page 265
  - "Resource state code values" on page 266
  - "Resource status modifiers (positions 4 and 5)" on page 282
  - "Resource status field information (positions 6–10)" on page 283
- "Session states and modifiers" on page 284
  - "Session state modifiers and suffixes" on page 284
  - "Session initiation states" on page 284
  - "Session termination states" on page 290
  - "Session status modifiers (positions 6–8)" on page 291

Resource status codes and modifiers

VTAM provides detailed information on the status of a resource. This status is defined by a state code that contains as many as 10 characters.

Note: The resource state code abbreviation might be truncated if optional status information is displayed in positions 4—10. For example, ACTIV is displayed if an LU is in an active state. If a session is queued, pending active, or active for this LU, the resource status modifier /S appears in positions 4 and 5, and ACTIV is truncated (ACT/S).

See "Resource status modifiers (positions 4 and 5)" on page 282 and "Resource status field information (positions 6–10)" on page 283 for additional information.

The status code abbreviation appears in some VTAM messages in response to a DISPLAY ID command. See z/OS Communications Server: SNA Operation for more information about the DISPLAY ID command and the messages issued by VTAM in response to this command.

Resource state code categories

The classification of states into the following major categories might aid in deciding if a problem exists. If problem determination is needed, see z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures.

Category
Meaning

Final
VTAM has no further processing to do for the node.

Short transient (Short)
The node is awaiting completion of an operation (such as I/O) that will take a relatively short time. If the node remains in this state for a long period of time, there is probably a hardware or software error.

Long transient (Long)
The node is awaiting completion of an operation that will take a relatively long time. If the node remains in this state for an unreasonable length of time, there is probably a hardware or software error.

© Copyright IBM Corp. 2000, 2021

Suspended (Susp)
This node is awaiting processing of another node. When the awaited processing is completed, the status of this node should change. If the awaited processing is completed and this node remains in this state, there is probably a software problem.

Internal (Int)
This state is used within VTAM to direct processing. It should never be displayed. If it is, there is probably a software problem.

Resource state code values

The first byte represents the resource-status categories:

Value (hex)	Current state category	Desired state category
00	Inactive	Inactive
01	Pending inactive	Not used
02	Connectable	Connectable
03	Reactivate	Reactivate
04	Pending active	Not used
05	Active	Active
06	Routable	Routable

The second byte of RPRCURST and RPRDESST gives the specific resource status. The following table shows the two bytes in combination (for example, value hexadecimal 0001 indicates a category of zero-zero and a specific code of zero-one).

Table 12. Resource state code values

Resource state	Value (hex)	Category	Resource status
ACTIV	0505	Final	The resource is in the active state.
APEER	0501	Final	Attach PU Type 4 or 5 (peer): The node is the backup link station to which a PU Type 4 or 5 in another domain is attached.
CONCT	0200	Final	Connectable: A VARY ACT command has completed for a switched physical or logical unit, or for an application program. 1. For switched resources, a dial-in or dial-out request will be honored, but the resource is not in use at this time. 2. For application programs, an OPEN ACB has not yet been issued.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
CTDER	041D	Susp	Contacted error: A node, such as a link station or physical unit, was being activated and the contacted request was received indicating the contacted error state. For a physical unit, a request to deactivate the resource has been scheduled. For a link station, if the NCP it is trying to contact is being activated, the link station activation will be suspended until the activation is completed; then the link station will be contacted again. A second CTDER causes deactivation of the link station.
CTD1	043D	Susp	Contacted(1): A link station was being activated, and received a contacted request from the appropriate PU services. Because the communication controller contacted is being activated, the activation of the link station is suspended until the communication controller has been activated. Activation processing for the link station is redriven after the communication controller has been activated.
CTRQI	043A	Susp	Contacted(2) request IPL: A node, such as a link station or a physical unit, is being activated, and the contacted request indicates that reload is required. For a physical unit, a request to deactivate the resource has been scheduled. For a link station, if the NCP it is trying to contact is being activated, the link station activation will be suspended until the communication controller has been activated. The link station will then be contacted again. A second CTRQI deactivates the link station.
CT1NS	040F	Susp	Contact(1) not sent: A link station reached the point in its activation where a contact request should be sent, but the NCP to be contacted is not in a suitable state. The link station activation is suspended and will be redriven when the NCP activation reaches the point where it can be contacted (when its state is PAPU2).
DALUC	011E	Susp	DACTLU complete: A DACTLU request was sent and the response was received, but some higher-level node recovery processing has started. This node will remain in this state until the higher-level process redrives it.
DAPUC	011F	Int	DACTPU complete: A DACTPU request was sent as the result of a force deactivate or force reactivate command, and either the response was received or, in the case of a communication controller, a route failed and a DACTPU request was received.
DEFND	0001	Short	Defined: A VARY ACT command is being processed for a major node. The major node and its subnodes are known to VTAM. The activation has been suspended while the processing of the command moves from one internal VTAM PAB to another.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
DLLDD	05	Final	Loaded: The physical unit requested a load and that load has been successfully completed.
DLPAB	04	Short	Pending load abort: The physical unit requested load cannot be completed; a request to cancel the load has been sent to the physical unit.
DLPLD	03	Long	Pending load: The physical unit is currently being loaded.
DLPRP	02	Short	Pending ACTPU response: An ACTPU request unit was sent to the physical unit, and VTAM is waiting for the ACTPU response by which the physical unit will indicate whether it needs to be loaded.
DLRST	01	Final	Reset: The physical unit is not being loaded.
DUMPC	011B	Susp	Dump complete: A link station was used to dump an NCP and the dump is complete, but the recovery or deactivation of the NCP has not reached the point where link stations connected to that NCP are processed. For recovery, that point is reached when the NCP load or dump procedure status is RESET. For a deactivation, that point is reached when the NCP status is PRSET.
FDSCC	0445	Int	Force Discontact completed: A discontact has been sent as a result of a force deactivate or force reactivate command, and the response to the discontact has been received.
HLACF	0409	Int	Higher-level activate failed: A node was being activated, and activation of its higher-level node failed. For example, a channel-attached physical unit or logical unit was being activated, and PUB allocation failed for its associated channel. A deactivate request was scheduled for the channel-attached physical unit or logical unit.
HLACT	042D	Int	Higher-level activate complete: A node is being activated and its higher-level node has completed activation. For example, a channel-attached physical unit or logical unit is being activated, and the activation of the associated channel has been completed. The activation of the resource is about to begin.
IINOP	0005	Final	Inactive (Inoperative): The resource has been deactivated by an INOP request or a forced deactivate request.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
INACS	0006	Final	Inactive with sessions: If the resource is a logical unit, the node is in the inactive state but might have active sessions. There is no LU-SSCP session, but the logical unit might have active LU-LU sessions. This state can occur when a cross-domain resource is made a same-domain resource as part of the takeover of the resources of an SSCP that failed. If the resource is a CDRM, the node is in an inactive state, but it supports active cross-domain LU-LU sessions. In this state, there is no SSCP-SSCP session, but the CDRM might be supporting active cross-domain LU-LU sessions. This state can occur when (1) the virtual route used by the SSCP-SSCP session is inoperative or has been deactivated by a DACTVR (FORCE), (2) activate CDRM contention has occurred, or (3) an unrecoverable error has been detected for the SSCP-SSCP session. The cross-domain active session, which used the SSCP-SSCP session to set up, remains intact.
INACT	0003	Final	Inactive: The resource has been deactivated.
INACX	0007	Final	Inactive with address transforms: An external CDRM could not be activated. A gateway NCP along the path to the CDRM did not have enough information to support a cross-network session with the CDRM.
INOP	0441	Susp	Inoperative: An INOP request, route failure, or force reactivate command is being processed. Active user sessions have been terminated. The resource is about to be reactivated, but must wait for a higher-level node to activate it.
INVAP	0417	Int	Activate PU response not valid: A node, such as a communication controller or physical unit, is being activated. The ACTPU request was sent, but the response is not valid. Two examples of responses that are not valid are (1) the response unit has a format that is not valid or indicates the physical unit is not in COLD or ERP state and (2) the resource has been loaded and the contents ID is not the expected value. A request to deactivate the resource was scheduled.
LLQED	043B	Susp	Lower-level queued: A VARY ACT command is being processed for a communication controller, and the RDT segment has just been built. The network names of both the major node and its subnodes are known to VTAM. At least one of the subnode link stations has been queued on another link station queue, because it is an operand of the RNAME=*keyword* on the second communication controller VARY ACT command. The activation of the communication controller has been suspended while the processing of the command moves from one internal VTAM PAB to another.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
NACDR	042F	Int	Negative Activate CDRM response: A CDRM is being activated and the activate CDRM request was sent, but the response was negative (the request failed). A request to deactivate the CDRM has been scheduled.
NACTL	0410	Int	Negative activate LU response: A node, such as an application program or other logical unit was being activated, and the activate LU request was sent, but the response was negative (the request failed). A request to deactivate the resource was scheduled.
NACTP	0412	Int	Negative activate PU response: A node, such as a communication controller or physical unit, was being activated and the activate PU request was sent, but the response was negative, and the request failed. A request to deactivate the resource was scheduled.
NADLK	0423	Int	Negative add link response: A channel link was being activated and an add link request was sent to the appropriate PU services. However, the response was negative and the request failed. A request to deactivate the resource was scheduled.
NADST	0420	Int	Negative add link station response: A channel link station was being activated and an add link station request was sent to the appropriate PU services. However, the response was negative and the request failed. A request to deactivate the resource was scheduled.
NALNK	0415	Int	Negative activate link response: A line was being activated, and the activate link request was sent, but the response was negative (the request failed). A request to deactivate the line has been scheduled.
NANNA	0431	Int	Negative allocate node network address: A node, such as a dynamically added physical unit or logical unit, was being activated, and the request network address assignment request was sent to the appropriate PU services, but the response was negative and the request failed. A request to deactivate the resource was scheduled.
NASNA	0426	Int	Negative allocate subnode network addresses: A node, such as a channel-attached or switched physical unit, is being connected and the request network address assignment request has been sent to the appropriate PU services. However, the response was negative and the request failed. A request to disconnect the resource was scheduled.
NCONO	0400	Int	Negative connect out response: A node, such as a channel-attached or switched physical unit, was being connected and the connect out request was sent to the appropriate physical unit services, but the response was negative and the request failed. A request to disconnect the resource was scheduled.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
NCONT	041C	Int	Negative contact response: A node, such as a link station or physical unit, was being activated and the contact request was sent, but the response was negative (the request failed). A request to deactivate the resource has been scheduled.
NEVAC	0004	Final	Never activated: The resource has never been activated.
NFRSV	0407	Int	Negative FRS control vector: All the frame relay physical units in a particular frame relay switching equipment set (FRSESET) were being activated, and the FRS control vector request was sent to the appropriate PU services. However, the response was negative, and the request failed. Requests to deactivate all the frame relay physical units in the FRSESET have been scheduled.
NLOAD	043C	Int	Negative load response: A communication controller was being activated and a load request was sent to the appropriate physical unit services, but the response was negative and the request failed. A request to deactivate the communication controller was scheduled.
NNAUV	0403	Int	Negative set NAU control vector: A node, such as a switched or dynamically added logical unit, was being connected and the set NAU control vector request was sent to the appropriate physical unit services, but the response was negative and the request failed. A request to disconnect the resource was scheduled.
NSARV	041A	Int	Negative set SAR control vector: A node, such as a link station, was being activated and the set SAR control vector request was sent to the appropriate PU services, but the response was negative and the request failed. A request to deactivate the resource was scheduled.
NSDT	0428	Int	Negative SDT response: A communication controller was being activated and the start data traffic request was sent, but the response was negative and the request failed. A request to deactivate the communication controller was scheduled.
NSNCP	042E	Int	Negative switch to NCP response: A PEP link was being activated, and the switch to NCP request was sent, but the response was negative and the request failed. A request to deactivate the PEP link was scheduled.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
NSSSV	0405	Int	Negative set SSS control vector: A node, such as a DR-added physical unit added by dynamic reconfiguration, or a switched physical unit, was being connected, and the set SSS control vector request was sent to the appropriate PU services, but the response was negative, and the request failed. A request to disconnect the node was scheduled.
NSTD	042A	Int	Negative set time and date response: A node, such as a communication controller, was being activated and the set time and date request was sent, but the response was negative and the request failed. A request to deactivate the node was scheduled.
NVYLM	0436	Int	Negative operator query (VFYLM) response: The resource was being activated and the response to the VTAM message IST361A was to terminate the NCP activation. A request to deactivate the resource has been scheduled.
PABCN	010B	Short	Pending abandon connection response: A node, such as a channel-attached or switched physical unit, is about to become disconnected. The abandon connection request has been sent to the appropriate PU services, but the response has not been received.
PABCO	0116	Short	Pending abandon connection out response: A node, such as a channel-attached or switched physical unit, is being disconnected and the abandon connect out request has been sent to the appropriate physical unit services, but the response has not been received.
PACDR	0430	Long	Pending activate CDRM response: A CDRM is being activated and the activate CDRM request has been sent, but the response has not been received.
PACTL	0411	Short	Pending activate LU response: A node, such as an application program or other logical unit, is being activated and the activate LU request has been sent, but the response has not been received.
PADLK	0421	Short	Pending add link response: A channel link is being activated and an add link request was sent to the appropriate PU services, but the response has not been received.
PADST	0419	Short	Pending add link station response: A channel-link station is being activated and an add link station request was sent to the appropriate PU services, but the response has not been received.
PALNK	0416	Short	Pending activate link response: A line is being activated, and the activate link request has been sent, but the response has not been received.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PALUC	0434	Short	Pending activate LU cleanup response: An active logical unit is undergoing recovery processing. An ACTLU request has been sent, but the response has not been received.
PANNA	0432	Short	Pending allocate node network address: A node, such as a dynamically added physical unit or logical unit, is being activated and the request network address assignment request has been sent to the appropriate PU services, but the response was not received.
PAPU1	0413	Short or Long	Pending activate PU(1) response: A communication controller is being activated, and might not need to be loaded. The ACTPU request was sent, but the response was not received. The sending of this request might have to wait for the availability of a virtual route. If one or more explicit routes are operative, this should be a short transient state while route activation proceeds. If no routes are operative, this might be a long transient state while VTAM waits for connectivity to be established along the route.
PAPU2	0425	Short or Long	Pending activate PU(2) response: A physical unit is being activated, did not need to be loaded or has been loaded, and the activate PU request has been sent, but the response has not been received. For a communication controller, the sending of this request might have to wait for the availability of a virtual route. If one or more explicit routes are operative, this should effectively be a short transient state while route activation proceeds. If no routes are operative, this might be a long transient state while VTAM waits for connectivity to be established along the route.
PASNA	0427	Short	Pending allocate subnode network addresses: A node, such as a channel-attached or switched physical unit, is being connected. The assign network address or request network address assignment request has been sent to the appropriate PU services, but the response was not received.
PBFSI	0448	Short	Pending BFSESSINFO: Takeover processing is in progress for an LU, and active sessions have not been completely reported to the SSCP.
PCDLA	0121	Short	Pending cleanup DACTLINK active: A VARY INACT,TYPE=FORCE command was entered for an NCP-attached line whose status is active, pending active, or pending inactive. The lower level nodes are being deactivated, and a DACTLINK (cleanup) request was sent for the line, but the response has not yet been received.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PCDLI	0122	Short	Pending cleanup DACTLINK inactive: A VARY INACT,TYPE=FORCE command was entered for an NCP-attached line whose status is not active, pending active, or pending inactive. A DACTLINK (cleanup) request was sent for the line, but the response has not yet been received.
PCONO	0401	Short	Pending connect out response: A node, such as a channel-attached or switched physical unit, is being connected and the connect out request has been sent to the appropriate PU services, but the response was not received.
PCON1	041E	Short	Pending contact(1) response: A node, such as a link station, is being activated, and the first contact request was sent to the appropriate PU services, but the response was not received.
PCON2	0422	Short	Pending contact(2) response: A node, such as a physical unit or link station, is being activated and the contact request (second attempt for link station) has been sent to the appropriate physical unit services, but the response has not been received.
PCTD1	041F	Long	Pending contacted(1) request: A node, such as a link station, is being activated, and the first contact response was received as a positive response, but the contacted request was not received. A communication controller will also be found in this state during activation while waiting for a link station connected to it to be activated. For CTC, if both sides are hung in PCTD1, enter VARY INACT,TYPE=FORCE then VARY ACT on one side only to bypass the problem.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PCTD2	0424	Long	Pending contacted(2) request: A node, for example, a link station or a physical unit, is being activated. The final contact request was sent by VTAM to the appropriate PU services and the response was received from the NCP, but the contacted request has not been received from the remote device. A communication controller will also be found in this state (it is a suspended state in this case) during activation while waiting for a link station connected to it to be activated. The difference between PCTD2 and PCTD1 is that a communication controller in the PCTD1 state might be loaded if a link station receives a contacted request indicating the NCP needs to be loaded, whereas in the PCTD2 state, both the link station and the NCP would be deactivated. **Note:** 1. When the remote device is a 3274, the most likely cause is the NRZI definition parameter. The NCP defaults to NRZI. If the NRZI definition parameter in the 3274 differs from that specified in the NCP, PCTD2 will result. 2. If a token-ring device connected to a SNA 3174 channel-attached controller is not logically and physically attached to the token ring at activation time, the device will remain in PCTD2 status until the device is made available. 3. A status of PCTD2 can be caused by an illegal cross-network activation attempt. 4. A status of PCTD2 can be caused by a bad cable at the local or remote device. Run the complete set of cable wrap tests at each location.
PDACL	010F	Short	Pending DACTLU response: A node, such as an application program or a logical unit, is being disconnected or deactivated. The DACTLU request has been sent, but the response has not been received.
PDACP	0110	Short	Pending DACTPU response: A node, such as a communication controller or physical unit, is being disconnected or deactivated. The DACTPU request has been sent, but the response has not been received.
PDANC	0442	Short	Pending DACTPU ANSC: A DACTPU request was sent to the resource, but the response has not been received. The resource was being activated when the automatic network shutdown complete (ANSC) RU was received from the NCP. This request causes the SSCP to reset the SSCP-PU session and then resume the activation procedure.
PDANS	0104	Short	The abandon connect in request unit has been sent for a node such as a switched link.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PDELR	010E	Short	Pending delete network resource response: A node, such as an application program, is being disconnected. The delete network resource request has been sent to the appropriate PU services, but the response has not been received.
PDGBK	0123	Short	Pending DACTLINK giveback: Records were lost when the VTAM subtask VTMTRACE was restarted. A VARY INACT,TYPE=GIVEBACK command was entered for an NCP attached line. A DACTLINK (giveback) request was sent for the line, but the response has not yet been received.
PDISC	010D	Short	Pending discontact response: A node, such as a link station or physical unit, is being deactivated or disconnected. The discontact request has been sent to the appropriate PU services, but the response has not been received.
PDLNK	0112	Short	Pending DACTLINK response: A line or channel-attached device is being deactivated, and the DACTLINK request has been sent to the appropriate PU services, but the response has not been received.
PDLUC	011D	Short	Pending Deactivate LU cleanup: An active logical unit is undergoing error-recovery processing and the DACTLU request has been sent, but the response has not been received.
PDMPC	0439	Long	Pending dump contention: VTAM is waiting for an indication from the communication controller to resume operation.
PDPA1	0443	Short	Pending DACTPU (ACT1): A DACTPU request was sent to the resource, but the response has not been received. The communication controller was being activated and was found already loaded. When the DACTPU response is received, this state is exited and processing continues from the beginning. Another attempt to load is allowed.
PDPA2	0444	Short	Pending DACTPU (ACT2): A DACTPU has been sent to the resource, but the response has not been received. If the resource is a physical unit Type 4, it was being activated and a load was performed. Once the DACTPU response is received, the activation of the communication controller will proceed. If the resource is a BSC 3270 physical unit, a general poll failure occurred and the DACTPU was sent to clean up internal control blocks. When the response is received, an ACTPU will be sent.
PFDCP	0440	Short	Pending force DACTPU response: A DACTPU has been sent as a result of a force-reactivate or force-deactivate command against a node, such as a communication controller. The response has not been received.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PFDLU	0120	Short	Pending force DACTLU response: A DACTLU has been sent as a result of a force-deactivate command for the logical unit, but the response has not yet been received.
PFDMP	0119	Short	Pending dump response: A dump is being performed on a communication controller over a link station, and it has not yet completed processing.
PFDSC	042C	Short	Pending force discontact response: A physical unit is being forced to deactivate or forced to reactivate and the discontact request has been sent to the appropriate PU services, but the response has not been received.
PFNNA	011C	Short	Pending free node network address: A node, such as a switched or dynamically added physical unit or logical unit, is being deactivated. The free network address request has been sent to the appropriate PU services, but the response has not been received.
PFRSV	042F	Susp	Pending FRS control vector response: A frame relay physical unit is being activated and one of the following situations has occurred: • The other physical units in the frame relay switching equipment set (FRSESET) have not received positive RNAA responses. • The FRS control vector request has been sent to the appropriate PU services, but the response has not been received.
PFSNA	010C	Short	Pending free subnode network addresses: A node, such as a channel-attached or switched physical unit, is being disconnected. The free network address request has been sent to the appropriate PU services, but the response has not been received.
PGAIN	0449	Long	Pending Enterprise Extender hostname resolution using the resolver API GetAddrInfo function. This state can vary in duration depending on many factors; for example, how long it takes for the resolver to resolve the hostname, or for the request to fail (either a timeout using resolver configuration definitions or by the IPRESOLV VTAM keyword), or for the TCP/IP stack being used for Enterprise Extender to become active.
PHLAC	040A	Susp	Pending higher-level activation: A node is awaiting activation of its higher-level node. For example, a channel-attached physical unit or logical unit is being activated, and the request to activate the associated channel (that is, the associated PUB) has not completed.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PHLIN	0102	Susp	Pending higher-level deactivation: A node is inactive and its higher-level node is being deactivated. For example, a channel-attached physical unit is inactive and the associated channel PUB is being deallocated.
PINAC	0100	Long	Pending inactive: CDRM is being deactivated.
PLOAD	040E	Long	Pending load: Either an NCP is being activated and a load operation has begun, or a peripheral physical unit, such as an 8775, is being activated, the physical unit has requested a load, and the SSCP sent the load request to an application program defined in the CNM routing tables. The physical unit has not received a response.
PLODC	043E	Long	Pending load contention: VTAM is waiting for an indication from the communication controller to resume operation.
PLSTC	043F	Long	Pending load station conditional: Activation processing for a communication controller is waiting for the link station over which the communication controller will be loaded to become available. When the link station is capable of being used for loading, if the link station is a channel link station, VTAM determines if the communication controller is loaded. If it is, a load is not done and activation proceeds. If it is not a channel link station, or if the communication controller is not loaded, a load is performed.
PLSTU	040D	Long	Pending load station unconditional: Activation processing for a communication controller will be loaded to become available. When the link station is capable of being used for loading, a load of the NCP will be done.
PMALD	0446	Long	Pending migration ACTPU load or dump procedure: An NCP session recovery loop has been suspended because of an ongoing load or dump operation.
PMATM	0447	Long	Pending migration ACTPU timer: An NCP is waiting for the expiration of a time interval before trying session activation again.
PNAUV	0404	Short	Pending set NAU control vector response: A node, such as a switched or dynamically added logical unit, is being connected, and the set NAU control vector request has been sent to the appropriate PU services, but the response has not been received.
PNFY1	0113	Long	Pending notify(1): A node, such as a logical unit, is being deactivated or disconnected. The request to terminate user sessions has been scheduled, but the notify request indicating that the user sessions have ended has not yet been received. For example, the application program did not issue CLSDST.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PNFY2	0108	Long	Pending notify(2): A node, such as a logical unit, is about to become connectable and the request to terminate any queued user sessions has been scheduled. However, the notify request indicating that the user sessions have ended has not yet been received.
PNFY3	0105	Long	Pending notify(3): A node is about to become inactive and the request to terminate queued user sessions has been scheduled. However, the notify request indicating that the user sessions have ended has not yet been received.
POAS1	0437	Long	Pending operator query (AUTOSYN1) response: A communication controller is being activated, and message IST183A, which asks if the communication controller should be reloaded or resynchronized, has been entered. The message was sent after the communication controller was contacted but before an SSCP-PU session was established. The reply was not received.
POAS2	0438	Long	Pending operator query (AUTOSYN2) response: A communication controller is being activated, and message IST183A, which asks if the communication controller should be reloaded or resynchronized, has been issued. The message was sent after an SSCP-PU session was established with the communication controller. The reply was not received.
PREQC	0402	Long	Pending request contact request: A node, such as a channel-attached or switched physical unit, is being connected and the connect out response has been received, but the request contact request has not been received.
PRMPO	0103	Short	Pending RMPO response: A remote power off request has been sent over a link station and the response has not been received.
PRSET	0101	Short	Pending reset: The resource is inactive, but the network name is still known to VTAM.
PSARV	041B	Short	Pending set SAR control vector response: A node, such as a link station, is being activated and the set SAR control vector request has been sent to the appropriate PU services, but the response has not been received.
PSDT	0429	Short	Pending start data traffic response: A node, such as a communication controller, was being activated, and the start data traffic request was sent, but the response was not received.
PSNCP	0414	Short	Pending switch to NCP response: A PEP link is being activated, and the switch to NCP request was sent, but the response has not been received.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PSSSV	0406	Short	Pending set SSS control vector response: A switched physical unit is being connected, or a dynamically added physical unit is being activated, and the set SSS control cector request has been sent to the appropriate PU services, but the response has not been received.
PSTD	042B	Short	Pending set time and date response: A communication controller was being activated, and the set time and date request was sent, but the response was not received.
PSUBD	0502	Susp	Pending subnode definition: The resource is active but is waiting for dynamic subnodes to be defined. If a switched line is in this state it cannot be used for dial out.
PSUBR	0504	Susp	Pending subnode release: An acquired communication controller that was activated before it was acquired is being released; that is, a request to release the subnodes in the unowned portion of the communication controller is in progress.
PSUB1	0115	Susp	Pending subnode deactivate(1): A node supporting subnodes, for example, an application program, communication controller, link, or physical unit, is being deactivated or disconnected. Terminate requests for user sessions for application programs or LUs are being performed.
PSUB2	010A	Susp	Pending subnode deactivate(2): A node supporting subnodes, for example, an application program, communication controller, link, or physical unit, is about to become connectable. Terminate requests for queued user sessions for application programs or LUs are being performed.
PSUB3	0107	Susp	Pending subnode deactivate(3): A node supporting subnodes, for example, an application program, communication controller, link, or physical unit, is about to become inactive. Terminate requests for queued user sessions that apply to application programs or LUs are being performed.
PSWEP	0111	Short	Pending switch to EP mode response: A PEP link has been deactivated. The switch to EP mode request has been sent to the appropriate PU services, but the response has not been received.
PTRM1	0114	Short	Pending terminate(1) response: A node, such as a logical unit, is being deactivated or disconnected. The request to terminate user sessions has been scheduled, but the response has not yet been received.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
PTRM2	0109	Short	Pending terminate(2): A node, such as a logical unit, is about to become connectable, and the request to terminate queued user sessions has been scheduled. However, the response has not yet been received.
PTRM3	0106	Short	Pending terminate(3) response: A logical unit is about to become inactive and the request to terminate queued user sessions has been scheduled, but the response has not yet been received.
PVYLM	0435	Long	Pending operator query (VFYLM) response: The resource is being activated and the VTAM operator message IST361A or IST937A has been issued, but the reply has not yet been received. Message IST361A asked the operator if he wanted to load the NCP or terminate the NCP activation. Message IST937A asked the operator if he wanted to reload the NCP, deactivate the NCP, or ignore the correlator mismatch.
P095A	0118	Long	Pending operator query response: An ERP has issued message IST095A asking whether an ERP dump is desired. The reply has not been received.
P284A	0408	Long	Pending operator query response: A communication controller is being recovered and message IST284A, asking whether the communication controller should be reloaded, has been issued. The reply has not been received.
RACTH	0301		Reactivate at higher level: The resource is being deactivated and, once inactive, will wait for its reactivation to be driven by a higher-level node. (This is a desired state only.)
RACTN	0300		Reactivate at this level: The resource is being deactivated and will then be reactivated at this level. (This is a desired state only.)
RADDF	0433	Int	RDTADD failed: A node was being activated and the request to add the associated network address to the VTAM RDTADD data base has failed. A request to deactivate the resource has been scheduled.
RDIAL	0201		Redial: A switched physical unit is being disconnected and an attempt to redial the physical unit will be made once disconnection is complete. (This is a desired state only.)
RDRSP	0124	Long	Pending RTP_deallocation response.
RELSD	0002	Final	Released: A physical unit has been released, or it exists in the unowned portion of an activated-before-acquired communication controller and has not yet been acquired.

Table 12. Resource state code values (continued)

Resource state	Value (hex)	Category	Resource status
RESET	0000	Final	Reset: VTAM built a control block to represent the resource, but the resource has not been added to the symbol table. The resource is not usable by VTAM. You might have a duplicate resource name. For NCP resources, you might need to issue a VTAM VARY ACQ command to acquire the resource before using it.
RINAC	0600	Long	Routable, inactive: A MODIFY LL2 command is being processed for an inactive, dynamically added physical unit. In order to process the command, a network address had to be obtained for the physical unit. When the LL2 test is terminated, the physical unit will be returned to the inactive state.
RRLSD	0601	Long	Routable, released: A MODIFY LL2 command is being processed for a released, dynamically added physical unit. In order to process the command, a network address had to be obtained for the physical unit. When the LL2 test is terminated, the physical unit will be returned to the released state.
TRACT	03	Final	Active: The trace indicated is active.
TRPAR	02	Short	Pending ACT TRACE: The trace is being activated and the ACTTRACE request has been sent to the appropriate PU services, but the response has not been received.
TRPDR	01	Short	Pending DACTTRACE: The trace is being deactivated and the DACTTRACE request has been sent.
TRRES	00	Final	Reset: The trace indicated is not active.
183AF	0418	Int	Operator query (AUTOSYNCH) failed: A request to issue message IST183A was scheduled, but the message could not be issued. Processing continues as if the reply were negative.
284AF	0407	Int	Operator query failed: A request to issue message IST284A has been scheduled, but the message could not be issued. Processing continues as if the reply were negative.

Note:

1. The state abbreviations are listed in alphabetical sequence.
2. An asterisk (*) is used to denote state values that may appear in a 1-byte field containing a load status. These values describe the progress of a load requested by the physical unit on an ACTPU response.
3. A double asterisk (**) is used to denote state values that may appear in a 1-byte field containing the line trace, GPT trace, or SIT trace status.

Resource status modifiers (positions 4 and 5)

The following status modifiers can appear in positions 4 and 5 of the state field. Only one modifier will be present at a time.

Table 13. Resource status modifiers	
Modifier	**Meaning**
/I	Persistent session recovery is in progress. This status modifier is used only for application resources.
/R	Persistent session recovery is pending. This status modifier is used only for application resources.
/S	A session is queued, pending active, or active for this logical unit, terminal, or application. See “Session states and modifiers” on page 284 for a description of these session initiation states.

Note: Because the abbreviation of the state code is truncated to three characters prior to adding the two-character status modifier, the characters that make the state code unique (the fourth and fifth characters) might be lost. For example, if the /I modifier is appended to PNFY1, PNFY2, or PNFY3, the new state code is PNF/I. It is not possible to determine the original state code in this situation.

Resource status field information (positions 6–10)

The following resource status information can appear in character positions 6–10 in the resource status field in VTAM messages.

If a character position is not used, a hyphen (-) is displayed. For example, **ACTIV--S--** is displayed if the logical unit or cross-domain resource (CDRSC) is in an active state and defined as a shadow resource.

Table 14. Resource status field information		
Resource information	**Character position**	**Meaning**
B	10	The link station is functioning as a backup for another link station (in certain migration situations).
C	8	DACTLINK GIVEBACK processing is being done for a LINE as a result of a VARY RELEASE GIVEBACK command issued for an NCP.
D	10	The resource has been added or moved using dynamic reconfiguration.
E	10	The link station or cross-subarea link has been explicitly activated.
F	10	The link station was implicitly activated as a backup.
G	10	The resource is a logical line.
I	10	The link station or cross-subarea link has been implicitly (or automatically) activated, as a result of activating a resource to which this link or link station is subordinate or adjacent. See z/OS Communications Server: SNA Operation for an explanation of using the RNAME operand or the U operand to automatically activate link stations.
L	8	An independent LU is using this PU as an adjacent link station.
M	6	Takeover is in progress for the PU.
N	7	The resource was not originally owned by the host processing the DISPLAY command.

Table 14. Resource status field information (continued)		
Resource information	**Character position**	**Meaning**
R	9	A test-resolve retry condition exists for a local area network active leased line. This condition indicates that VTAM LAN support is sending test LPDUs to a station to resolve a route and will continue to do so until either the station is active or the operator deactivates the line.
S	8	The logical unit or cross-domain resource (CDRSC) is defined as a shadow resource. See z/OS Communications Server: SNA Network Implementation Guide for more information.
T	10	The resource (link, physical unit, or logical unit) is attached through the programmed resource capability (NTO) of the NCP.
W	8	The physical unit is defined with ALLOWACT=YES.
X	9	The resource was dynamically created.
Y	10	The cross-domain resource (CDRSC) was created dynamically.

Session states and modifiers

This section lists all session states and session status modifiers issued in DISPLAY SESSIONS and DISPLAY ID commands.

Session state modifiers and suffixes

Session states can be followed by one or more session status modifiers or by a session state suffix of -P or -S.

Session status modifiers

Session status modifiers appear in positions 6–8 of the session state.

Note: Part of the session state might be truncated if a modifier is present. For example, if code PDSRLST is issued with status modifier /C, VTAM displays **PDSRL/C**. Because the first five characters of session states are unique, it is still possible to identify the original session state.

See “Session status modifiers (positions 6–8)” on page 291 for a listing of possible session status modifiers.

Session state suffixes (-P and -S)

If the session state is displayed with a suffix of -P, for example ACTIV-P, the resource is the primary LU.

If the session state is displayed with a suffix of -S, for example ACTIV-S, the resource is the secondary LU.

Session initiation states

A session state can be classified into one of the following three groups:

- **Q (Queued)**
  - If the session state is preceded by **A-**, the session is traversing the APPN portion of the network. The session is considered queued when the session request has been received at a node performing only APPN functions for this session.

– For all other states, the session is considered queued under the following circumstances:
  - A session request has been received, but session establishment has not located the resources required for the session.
  - The resources required for the session have been located; however, the resources are temporarily unavailable for sessions. Further session establishment procedures have been suspended until the resource is available. The session is in a reallocation-pending state.

- **P/A (Pending Active)**
- A session is considered to be pending active when both resources required for session setup have been successfully located and are available for sessions. Session establishment proceeds.
- **ACT (Active)**

  A session is considered active (ACT) when all session start signals have been received, and a session has been successfully established.

The following table lists possible session states.

Note: If the session state is preceded by **A-**, the session is traversing the APPN portion of the network.

Table 15. Session initiation states

Session state	Status	Meaning
A-PCOS	Q	Pending COS reply.
A-PCRYPT	Q	Pending cryptographic keys.
A-PDS	Q	VTAM has an APPN locate chain for the session. A search might be in progress or completed, but the session is not fully active yet. To determine the complete status of the session, use the SID and LU names from the message to find the LUs and session in this and other hosts.
A-PNCOSM	Q	Pending entry COS mapping.
A-PRSCV	Q	Pending RSCV reply.
A-PSACF	Q	Pending subarea chain flow.
A-PSAR	Q	Pending Subarea reply.
A-PTGVS	Q	Pending TG reply.
A-PXCOSM	Q	Pending exit COS mapping.
A-QUEUE	Q	This LU-LU session is queued. One of the LUs is at its session limit or is not available. If this VTAM is functioning as an APPN network node server and is not doing any subarea routing, this state is the only queued state that is displayed. If this VTAM does subarea routing, in either a pure subarea or mixed APPN/subarea network, one of the other queued session states listed in this table will be displayed.
A-RESET	Q	The session is reset.
A-TERM	P/A	The session is pending termination.
ACTIV	ACT	The session is active. A session has been successfully established.
ADIALIP	P/A	Dial in progress for APPN LU.

Table 15. Session initiation states (continued)

Session state	Status	Meaning
CDPRIP	Q	CDINIT pending cross-domain routing completion. Another request is pending for the specified LU, and this session will wait for routing to complete.
DDIALIP	Q	Dial in progress for DLU. A session will stay in DDIALIP until the DIAL START process completes. This process includes completing the connection and activating the PU and its subordinate resources. The length of time a session stays in DDIALIP is dependent upon the network configuration.
DLUCOMP	Q	DLU direction processing complete.
DLUPROR	Q	DLU direction processing required.
DLURNAA	Q	DLU direction RNAA processing needed.
DNOTFYNN	Q	Destination notification not necessary
DRNASUS	Q	DLU direction RNAA processing suspended pending termination using same PLU network address.
DSSPD	Q	DSRLST pending cross-domain routing in progress. The DSRLST will be sent when routing is complete for the previous request.
INITC	Q	The SIB has been initialized.
INITSENT	Q	INIT or CDINIT response has been sent.
NULL	Q	Initial state of session.
ODIALIP	Q	Dial in progress for the OLU.
OLUEC	Q	OLU endpoint processing complete.
OLUCOMP	Q	OLU direction processing complete.
OLUEN	Q	OLU endpoint domain processing needed.
OLUPROR	Q	OLU direction processing required.
OLURNAA	Q	OLU direction RNAA processing needed.
ORNASUS	Q	OLU direction RNAA processing suspended pending termination of a session using same PLU network address.
PADIAL	P/A	Pending dial response for APPN LU.
PARAMRU	P/A	Pending APPN LU address assignment. A network address was needed for one of the LUs. VTAM has either sent an RNAA to the boundary function that owns the adjacent link station for one of the LUs or has sent a CDINNIT format 5 to the SSCP at the end of a VRTG and is waiting a response.
PARSCV	P/A	Pending APPN RSCV calculation for SLU initiated sessions.
PBFCINIT	P/A	Pending BFCINIT response.
PBIPLUBF	P/A	Pending receipt of the BFINIT from the boundary function of the APPN PLU.

Table 15. Session initiation states (continued)

Session state	Status	Meaning
PBISLUBF	P/A	Pending receipt of the BFINIT from the boundary function of the APPN SLU.
PCDCQ	Q	Pending CDCINIT request. This state is set when the SSCP(PLU) has sent or received CDINIT response and is waiting for the SSCP(SLU) to send CDCINIT. If a CDCINIT arrives before this state is reached, the CDCINIT is queued with no state change.
PCDCS	P/A	Pending CDCINIT response.
PCDDQ	Q	Pending CDINITDQ response. This state is set when the session was reallocated and a CDCINIT DQ request was sent.
PCDINIT	Q	Pending CDINIT response.
PCFRES	Q	Pending generic resource resolution for destination LU (DLU).
PCFUPD	Q	Pending coupling facility update for origination LU (OLU).
PCINIT	P/A	Pending CINIT or BFCINIT response.
PCIST	P/A	Pending CINIT or BFCINIT response and session start has already been received.
PCRCQ	Q	Pending cryptographic response for CDINIT request.
PCRCS	Q	Pending session cryptographic key for CINIT response.
PCRDQ	Q	Pending session cryptographic key for DEQUEUE request.
PCRDS	Q	Pending session cryptographic key for DEQUEUE response.
PCRYPK	Q	Pending cryptographic keys.
PDDIAL	Q	Pending dial response for the DLU.
PDLUIO	Q	Pending USS message response in DLU direction. The DLU device must respond to the USS message or no sessions will be initialized.
PDNETDET	Q	Pending DSRLST response for determination of the network identifier of the destination LU. A DSRLST has been sent for another session.
PDRAMRU	Q	DLU pending response from address manager for a request.
PDRDS	Q	Pending resource discovery search (RDS) completion.
PDRNAAD	Q	DLU RNAA response pending from the gateway NCP in the OLU direction.
PDSRHPR	Q	Pending DSRLST response with the outbound PU address for a VRTG connection.
PDSRLST	Q	Pending direct search list Type 01 and 02 response. These types of direct search are sent from the SSCP (OLU) when an autologon session establishment is in progress between a dial SLU and a cross domain PLU, or when a DSRLST is sent for NETID determination.

Table 15. Session initiation states (continued)		
Session state	**Status**	**Meaning**
PNOTIFYA	P/A	Pending NOTIFY(A) for VRTG.
PODIAL	Q	Pending dial response for OLU.
POLUIO	Q	Pending USS message response in OLU direction. The OLU device must respond to the USS message or no sessions will be initialized.
PORAMRU	Q	OLU pending response from address manager for a request.
PORNAAO	Q	An RNAA response is pending from gateway NCP in the OLU direction.
POSACOM	Q	Pending override session address (OSA) completion. This state is set when a session is initiated to a non-SNA SLU, and a previous session with the SLU is terminated.
PPCQRPY	Q	Pending PCID_QUERY_REPLY IPS from the APPN side of the node.
PRAV1	Q	Pending resource available. A resource was found during OLU processing that was unavailable. Session setup will continue when the LU becomes available.
PRAV2	Q	Pending resource available. A resource was found during DLU processing that was unavailable. Session setup will continue when the LU becomes available.
PRAV3	P/A	Status checking found an APPN logical unit PU temporarily unavailable. Session setup will wait on the PU to become available.
PREALC	Q	Pending reallocation. A session has been queued.
PRECOVRY	P/A	Pending completion of multinode persistent session recovery processing.
PRMRC	Q	Pending request multiple routes inter-process signal (IPS) for CDINIT.
PRMRD	Q	Pending request multiple routes inter-process signal (IPS) for DSRLST.
PRSCDPRE	Q	Pending RSCV precalculation for the DLU.
PRSCOPRE	Q	Pending RSCV precalculation for the OLU.
PRSCVD	Q	Pending RSCV in the DLU direction.
PRTPSTR	P/A	Pending RTP start.
PSCRYP	Q	Pending send of the cryptographic control vector by the primary XRF session.

Table 15. Session initiation states (continued)

Session state	Status	Meaning
PSEST	P/A	Pending SESSST or BFSESSST request. The session can be expecting any of several signals. Use D NET,SESSIONS,SID= command to see specific signals needed. **Note:** In storage situations, if you do not receive the started signal, it might be because the session is already active.
PSETCVR	Q	Pending SETCV response.
PSHRP	Q	Pending request single hop route reply.
PSLUIO	Q	Pending USS message response in SLU direction. The SLU device must respond to the USS message or no sessions will be initialized.
PSSADR	Q	Pending set session address (SSA) response. SSA is sent as part of initiation when the SLU is a non-SNA LU and not in the same domain.
PSWAP	P/A	Pending swap from hidden CDRSC to real CDRSC.
PTAKOVER	Q	Pending SSCP takeover is complete.
PTCRXCRS	Q	Pending translation of cryptographic keys for the CDINIT response for an XRF backup session.
PTCRYP	Q	Pending translation of cryptographic keys for the backup XRF session.
PXASL	Q	Pending associated LU name translation
PXDA1CDI	Q	Pending DLU alias to real translation. This SSCP located a USERVAR for the DLU and is attempting to translate the DLU real name into an alias name.
PXDA2CDT	Q	Pending DLU alias to real translation. Another SSCP located a USERVAR for the DLU and returned the value as a real name to this SSCP. VTAM is attempting to translate this real name into an alias name.
PXDA3DSL	Q	Pending DLU alias to real translation. During DSRLST response processing, VTAM is attempting to translate the DLU real name into an alias name.
PXDGC	Q	Pending DLU direction COS translation.
PXDLO	Q	Pending DLU logon mode translation.
PXDRD	Q	Pending DLU real name translation.
PXOGC	Q	Pending OLU direction COS translation.
REALCOM	Q	Reallocation complete.
REALIP	Q	Reallocation in progress. The session is currently being reallocated.
SETCVCOM	Q	SETCV complete.

Table 15. Session initiation states (continued)		
Session state	**Status**	**Meaning**
SEIPRT	Q	SESSEND in progress during routing. Routing will continue when the previous session completes termination.
SEOIP	Q	SESSEND processing in progress in OLU domain. A duplicate session exists, and this session will be suspended until termination processing has completed for the duplicate session.
UNKNOWN	Q	The session state could not be determined.

Session termination states

Termination states that follow are set during termination processing of a session:

NULL
The initial state. Termination is not in progress.

OSARECV
OSA response received.

PBFCLN
Pending BFCLEANUP response.

PCDTM
Pending CDTERM response. This is CDTERM sent for termination.

PCLNP
Pending CLEANUP response.

PCTMR
Pending CTERM response.

PINITO
Pending initiation I/O completion.

PLUIO
Pending USSMSG response from the SLU. A USSMSG was sent to the SLU and VTAM is waiting for a response. The termination of this session will complete when the device responds.

PLUCIO
USSMSG response from the SLU has been received and the session termination is continuing.

PMRCVTRM
Pending multinode persistent session recovery termination signal.

PSESEND
Pending SESSEND or BFSESSEND. The session can expect any of several session end signals. Use D NET,SESSIONS,SID command to see specific signals needed.

Note: Pending session end can also occur as a result of session outage notification processing when pre-V3R2 SSCPs are involved in the session setup even though the session might not currently be in termination.

PSESF
Pending CDSESSSF response.

PSETF
Pending CDSESSTF response.

POSAR
Pending override session address (OSA) response. An OSA request was sent to the non-SNA SLU requesting termination.

UNKNOWN
The session state could not be determined.

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 6. VTAM wait state event codes and IDs

Wait state event codes and IDs are used to determine why VTAM is in a wait state.

SSCP, PU services, LU services, and network operator services processes that are in wait states are represented by a waiting request element (WRE) queued off the LQAB of the subcomponent that controls the waiting process. The WRE for a process contains a 2-byte event code that identifies the event so you do not have to look at the event ID itself.

See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for an overview of the wait procedure.

Codes 0102–010C (configuration services LQAB group)

Wait state event codes and IDs associated with the configuration services miscellaneous command LQAB group and their meanings are as follows:

Event Code 0102

Explanation

Configuration services is waiting for an NCP to become active. Parameter *xxx...xxx* is the 6-byte NCP network address.

Event ID:
EIDCNACT

Event Format:
xxxxxxxxxxxx

Event Code 0103

Explanation

Configuration services is waiting for a link to become active. Parameter *xxx...xxx* is the 6-byte NCP network address, parameter *yyy...yyy* is the 6-byte link network address.

Event ID:
EIDCLACT

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0000

Event Code 0104

Explanation

Configuration services is waiting for the response to an activate or deactivate connect in request (for a VARY ANS command). Parameter *xxx...xxx* is the 6-byte NCP network address. Parameter *yyy...yyy* is the 6-byte link network address.

Event ID:
EIDCCIRS

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0001

© Copyright IBM Corp. 2000, 2021

Event Code 0105

Explanation

Configuration services is waiting for the response to an activate generalized PIU trace or a deactivate generalized PIU trace request. Parameter *xxx...xxx* is the 6-byte NCP network address; Parameter *yyy...yyy* is the 6-byte trace-resource network address (a PU, LU, Line, or NCP for GPT); Parameter *zzzzzz* is the 3-byte SNA request code of the activate/deactivate trace RU; Parameter *aa* is the 1-byte trace RU type byte.

Event ID:
EIDCTRRS

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy zzzzzz aa

Event Code 0106

Explanation

Session services is waiting for an LU to become stable (for example, for error recovery to be completed) so that a session may be set up. Parameter *xxx...xxx* is the 8-byte network name of the LU.

Event ID:
EIDCSTBL

Event Format:
0000 *xxxxxxxxxxxxxxxx*

Event Code 0107

Explanation

Configuration services is waiting for the response to an activate or deactivate NETCTLR request. Parameter *xxx...xxx* is the 16-byte activate or deactivate trace ID (EIDCTRRS). Parameter *yyy...yyy* is the 8-byte name of the line.

Event ID:
EIDCTNRS

Event Format:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx yyyyyyyyyyyyyyyy

Event Code 0108

Explanation

Configuration services is waiting for the response to an RNAA for an independent LU when processing and ACT trace command. Parameter *xxx...xxx* is the 8-byte name of the LU resource. Parameter *yyyyyy* is the 3-byte SNA request code for RNAA.

Event ID:
EIDCTRNA

Event Format:
xxxxxxxxxxxxxxxx yyyyyy

Event Code 010A

Explanation

Checkpoint datasets are waiting for ISTPDCLU close to complete.

Event ID:
EIDCCKPT

Event Format:
CHKPT

Event Code 010B

Explanation

Configuration services agent is waiting for a DSRLST response. Parameter *xx...xx* is the 8-byte resource netid value requested by the agent. Parameter *yy...yy* is the 8-byte resource name requested by the agent. Parameter *zzz...zz* is the 8-byte PCID sent on the DSRLST request.

Event ID:
EIDDSIDC

Event Format:
010B *xxxxxxxx yyyyyyyy zzzzzzzz*

Event Code 010C

Explanation

Configuration services agent is waiting for the TCP/IP to be able to perform resolver function. Parameter *xx...xx* is the 8-character group name. Parameter *yy...yy* is the 6-character link network address. Parameter *zzz...zz* is the 8-character link name.

Event ID:
EIDTAIDC

Event Format:
010C *xxxxxxxx yyyyyyyy zzzzzzzz*

Codes 0201–020D (I/O LQAB group)

Wait state event codes and IDs associated with the I/O LQAB group and their meanings are as follows:

Event Code 0201

Explanation

The requester (with 6-byte network address *xxx...xxx*) is waiting for the response to a normal-flow request unit sent to the resource having the 6-byte network address *yyy...yyy*. Parameter *aaaaaaaa* is the 4-byte CPCB operation code corresponding to the RU type. Parameter *zzzz* is the 2-byte sequence number of the request unit.

Event ID:
EIDINFRS

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0201 *aaaaaaaa zzzz*

Event Code 0202

Explanation

The requester (with 6-byte network address *xxx...xxx*) is waiting for the response to an expedited-flow request unit sent to the resource having the 6-byte network address *yyy...yyy*. Parameter *aaaaaaaa* is the 4-byte CPCB operation code corresponding to the RU type. Parameter *zzzz* is the 2-byte sequence number of the request unit.

Event ID:
EIDIEFRS

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0202 *aaaaaaaa zzzz*

Event Code 0203

Explanation

Management services is waiting for a record storage request from an NCP as part of the DISPLAY STORE command. Parameter *xxx...xxx* is the 6-byte SSCP network address. Parameter *yyy...yyy* is the 6-byte NCP network address. Parameter *zzzz* is the 2-byte procedure relation ID (PRID).

Event ID:
EIDIRCRU

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0203 *zzzz*

Event Code 0204

Explanation

Logical unit services is waiting for the response to an UNBIND request unit. Parameter *xxx...xxx* is the 6-byte network address of the LU sending the request. Parameter *yyy...yyy* is the 6-byte network address of the LU to which the request was sent.

Event ID:
EIDIURSP

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0204

Event Code 0206

Explanation

Configuration services (with 6-byte SSCP network address *xxx...xxx*) is waiting for a RECSTOR RU from the NCP (with 6-byte network address *yyy...yyy*) as part of MODIFY DUMP processing. Parameters *aaaaaaaa* and *llll* are the address and the length of the NCP storage being requested.

A *vv* of:

04 indicates a dynamic NCP dump
05 indicates a MOSS dump
06 indicates a CSP dump
07 transfer NCP dump header
08 transfer NCP dump main storage
09 indicates display disk

Event ID:
EIDIRSTO

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0206 *vv aaaaaaaa llll*

Event Code 0208

Explanation

Session services (with 6-byte SSCP network address *xxx...xxx*) is waiting for SESSEND to be received from an LU (with 6-byte network address *yyy...yyy*) or for CDSESSEND to be received from a CDRM (network address *yyy...yyy*) so that the control blocks associated with the session may be freed and the LUs may be reallocated. Parameter *aaa...aaa* is the 8-byte name of the network in which the address is known. Parameter *zzz...zzz* is the 8-byte PCID associated with the session.

Event ID:
EIDISEND

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0208 *aaaaaaaaaaaaaaaa zzzzzzzzzzzzzzzz*

Event Code 0209

Explanation

The PVI subcomponent is waiting to be posted by TSC when an I/O operation has been scheduled. The 6-byte fields, *xxx...xxx* and *yyy...yyy*, are the network addresses of the originator and destination of the request unit. Parameter *aaaaaaaa* is the 4-byte CPCB operation code corresponding to the RU type. Parameter *zzzzzzzz* is the address of the TSCB for the to-be-posted operation.

Event ID:
EIDIIOSC

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 0209 *aaaaaaaa zzzzzzzz*

Event Code 020B

Explanation

Session services (SSCP network address *xxx...xxx*) is waiting for an override session address (OSA) RU for the non-SNA logical unit (6-byte network address *yyy...yyy*) to be completed.

Event ID:
EIDIOSAR

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 020B

Event Code 020C

Explanation

Session services is waiting for a response from a device LU. Parameter *xxx...xxx* is the 6-byte SSCP network address. Parameter *yyy...yyy* is the 6-byte network address for the device LU.

Event ID:
EIDIOREQ

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 020C

Event Code 020D

Explanation

Configuration services is waiting for a response to a SETCV(FRS) request.

Event ID:
EIDIFRSE

Event Format:
xxxxxxxxxxxx yyyyyyyyyyyy 020D *aaaaaaaaaaaaaaaa*

Codes 0301–0306 (logical unit services LQAB group)

Wait state event codes and IDs associated with the logical unit services service manager LQAB group and their meanings are as follows:

Event Code 0301

Explanation

Logical unit services is waiting for a CINIT RU from the SSCP to satisfy an OPNDST ACCEPT request. Parameter *xxx...xxx* is an 8-byte primary LU name and parameter *yyy...yyy* is either an 8-byte secondary LU name (for OPNDST ACCEPT SPECIFIC) or is binary zeros (for OPNDST ACCEPT ANY).

Parameter *z* is either **Y** or **N**.

- **Y** indicates the request specified a bind-image override.
- **N** indicates the request did not specify a bind-image override.

Parameter *www...www* is the 8-byte network identifier for the SLU.

Event ID:
EIDLACPT

Event Format:
xxxxxxxxxxxxxxxx 0301 ACCEPT *yyyyyyyyyyyyyyyy wwwwwwwwwwwwwwww z*

Event Code 0302

Explanation

LU services is waiting for a CINIT RU from the SSCP to satisfy an OPNDST ACQUIRE request. Parameter *xxx...xxx* is an 8-byte primary LU name and parameter *yyy...yyy* is the nine-byte user-request correlator used to correlate the CINIT to the particular OPNDST ACQUIRE request.

Event ID:
EIDLAQIR

Event Format:
xxxxxxxxxxxxxxxx 0302 ACQUIRE *yyyyyyyyyyyyyyyyyy*

Event Code 0304

Explanation

Logical unit services is waiting for a VTAM operator message to be received so that a queued RCVCMD from a programmed operator application request can be completed. Parameter *xxx...xxx* is the 8-byte network name of the application program.

Event ID:
EIDLRCVC

Event Format:
xxxxxxxxxxxxxxxx 0304 RCVCMD

Event Code 0305

Explanation

Logical unit services (for a secondary logical unit with 6-byte network address *xxx...xxx*) is awaiting the receipt of a CRV request unit from the primary logical unit (with 6-byte network address *yyy...yyy*) so that OPNSEC macro processing can be completed. Parameter *bbbbbbbbbb* is a 5-byte field of blanks (X'4040404040').

Event ID:
EIDLCRV

Event Format:
CRV*bbbbbbbbbb* 0305 *xxxxxxxxxxxx yyyyyyyyyyyy*

Event Code 0306

Explanation

Logical unit services is waiting for a CRYPTO key translation during OPNSEC processing. Parameter *xxx...xxx* is the 8-byte application name. Parameter *yyy...yyy* is the 6-byte primary network address and parameter *zzz...zzz* is the 6-byte secondary network address.

Event ID:
EIDLTRK

Event Format:
xxxxxxxxxxxxxxxx 0306 TRKEY *yyyyyyyyyyyy zzzzzzzzzzzz*

Codes 0401–0409 (physical unit services LQAB group)

Wait state event codes and IDs associated with the physical unit services LQAB group and their meanings are as follows:

Event Code 0401

Explanation

Physical unit services is waiting for an ongoing process to be completed so that another request may be processed. Parameter *xxxx* is the 2-byte element address of the (channel) link.

Event ID:
EIDPPCMP

Event Format:
0000 *xxxx*

Event Code 0402

Explanation

Physical unit services is waiting for the LUCB associated with an application program to be freed so that close ACB processing can complete. Parameter *xxxx* is the 2-byte element address of the application program.

Event ID:
EIDPFLUC

Event Format:
xxxx FREELUCB

Event Code 0403

Explanation

The OPEN/CLOSE subcomponent is waiting for the pending and queued active sessions to be terminated during a persistent close. Parameter *xxxx* is the 2-byte element address of the application program.

Event ID:
EIDPTERM

Event Format:
xxxx PENDTERM

Event Code 0404

Explanation

Physical unit services is waiting for CLOSE ACB processing for all application programs to be completed so that HALT processing for VTAM can be completed.

Event ID:
EIDPVHLT

Event Format:
VTAM HALT

Event Code 0405

Explanation

Physical unit services is waiting for ACTLU to be received from the SSCP so that OPEN ACB processing can be completed for an application program. Parameter *xxx...xxx* is the 8-byte network name of the application program.

Event ID:
EIDPACT

Event Format:
xxxxxxxxxxxxxxxx ACTIVATE

Event Code 0406

Explanation

Physical unit services is waiting for DACTLU to be received from the SSCP so that CLOSE ACB processing can be completed for an application program. Parameter *xxx...xxx* is the 8-byte network name of the application program.

Event ID:
EIDPDACT

Event Format:
xxxxxxxxxxxxxxxx DEACTIVATE

Event Code 0407

Explanation

Physical unit services is waiting for allocation or deallocation of a link to complete so that DACTLINK processing may complete. Parameter *xxxx* is the 2-byte element address of the link being allocated or deallocated.

Event ID:
EIDPADDV

Event Format:
xxxx LK AL DEAL

Event Code 0408

Explanation

The OPEN/CLOSE subcomponent is waiting for physical unit services to resume processing a delete network resource (DELETENR) request before continuing with a CLOSE ACB request. Parameter *xxxxxxxx* is the 4-byte LUCB storage address for which a CLOSE ACB is in progress.

Event ID:
EIDPDNRR

Event Format:
xxxxxxxx DELETENR RESUME

Event Code 0409

Explanation

Physical unit services is waiting for disabled transmission subsystem component (TSC) code to finish processing a logical unit control block (LUCB) before deleting it. Parameter *xxxxxxxx* is the 4-byte LUCB storage address TSC is processing.

Event ID:
EIDPCDER

Event Format:
xxxxxxxx CIDCTL DELETE

Codes 0501–0503 (network operator services LQAB group)

Wait state event codes and IDs associated with the network operator services LQAB group and their meanings are as follows:

Event Code 0501

Explanation

Network operator services is waiting for a RECSTOR RU to be received from an NCP as a part of D NCPSTOR or D DISK command processing. Parameter *xxx...xxx* is the 8-byte network name of the NCP and parameters *aaa...aaa* and *llll* are the address and the length of the NCP storage being displayed. Parameter *tt* is the 1-byte event ID type code.

Event ID:
EIDNNORS

Event Format:
xxxxxxxxxxxxxxxx 000000 *aaaaaaaa llll tt*

Event Code 0502

Explanation

Network operator services is waiting for a RECTRD RU to be received from an NCP as a part of MODIFY LL2 command processing. Parameter *xxx...xxx* is the 8-byte network name of the NCP, and parameter *yyyy* is the 2-byte procedure relation ID (PRID) associated with the request.

Event ID:
EIDNRTR

Event Format:
xxxxxxxxxxxxxxxx yyyy

Event Code 0503

Explanation

Network operator services is waiting for the operator to reply to a WTOR (IST1660A) with the password required for a DISPLAY APING command to complete. Parameter *xxx...xxx* is the 8-byte resource name entered on the ID parameter on the DISPLAY APING command and parameter *yyy...yyy* is the 8-byte NETID of that resource. Parameter *zzz...zzz* is the hexidecimal time message IST1660A was issued.

Event ID:
EIDNPING

Event Format:
xxxxxxxxxxxxxxxx yyyyyyyyyyyyyyyy 08 zzzzzzzzzzzzzzzz

Codes 0601–0610 (session services LQAB group)

The wait state event codes and IDs associated with the session services miscellaneous LQAB group and their meanings are as follows:

Event Code 0601

Explanation

Session services has suspended processing of an RU pending completion of another event. When the other event is completed, the RU will be processed.

This can occur for one of the following reasons:

- A CDCINIT has been received in a gateway SSCP, and SETCV processing has not completed.
- A CDCINIT was received, and cryptographic processing has not completed.
- A duplicate session information block (SIB) or direct search list SIB (DSSIB) was found having a lower PCID procedure resubmit number than the input request.
- A CDINIT DQ was received before the response to CDINIT QUEUED.
- A CDSESSST was received before the CDCINIT response.

Parameter *xxx...xxx* is the 8-byte PCID associated with the session.

Event ID:
EIDSIDEQ

Event Format:
0601 *xxxxxxxxxxxxxxxx*

Event Code 0602

Explanation

Session services is waiting for a CDINIT RU to be routed to the next SSCP in the session initiation path. Parameter *xxx...xxx* is the eight-character network ID of the next SSCP, and parameter *yyy...yyy* is the eight-character name of the LU.

Event ID:
EIDSINIT

Event Format:
0602 *xxxxxxxxxxxxxxxx yyyyyyyyyyyyyyyy*

Event Code 0603

Explanation

Session services is waiting for the completion of CDRM activation. Parameter *xxx...xxx* is the 8-byte name of the CDRM.

Event ID:
EIDECDIN

Event Format:
0603 *xxxxxxxxxxxxxxxx*

Event Code 0604

Explanation

Session services is waiting for a previous dial to complete. Parameter *xxx...xxx* is the 8-byte symbolic name of the PU. Parameter *zzz...zzz* is an 8-byte hexadecimal procedure correlation ID (PCID) associated with the LU-LU session.

Event ID:
EIDCDIAL

Event Format:
0604 DIAL *xxxxxxxxxxxxxxxx zzzzzzzzzzzzzzzz*

Event Code 0605

Explanation

CDTAKEDOWN Complete RU will be sent to notify the SSCP when all sessions using the specified SSCP have been terminated. Parameter *xxx...xxx* is the 8-byte name of an external SSCP.

Event ID:
EIDCDTAK

Event Format:
0605 *xxxxxxxxxxxxxxxx*

Event Code 0606

Explanation

Session services is waiting for CDSESSEND because a PLU that initiated a session request has duplicated the network address pair of a terminating session. Parameter *xxx...xxx* is the 8-byte network identifier for

the PLU and parameter *yyy...yyy* the 6-byte network address for the PLU. Parameter *zzz...zzz* is the 8-byte PCID associated with the terminating session.

Event ID:
EIDICDSE

Event Format:
0606 *xxxxxxxxxxxxxxxx yyyyyyyyyyyy zzzzzzzzzzzzzzzz*

Event Code 0607

Explanation

Session services is waiting to obtain a cryptographic key for the session. Parameter *xxx...xxx* is the 8-byte PCID associated with the session.

Event ID:
EIDCRYPY

Event Format:
0607 *xxxxxxxxxxxxxxxx*

Event Code 0608

Explanation

Session services is waiting for a SESSST for an XRF primary session with cryptographic information so that XRF backup session initiation is resumed. Parameter *xxx...xxx* is the 8-byte XRF SLU name.

Event ID:
EIDSXRCS

Event Format:
0608 *xxxxxxxxxxxxxxxx*

Event Code 0609

Explanation

Session services is waiting to obtain a cryptographic key for an XRF backup session. Parameter *xxx...xxx* is the 8-byte PCID for the session.

Event ID:
EIDSXCRT

Event Format:
0609 *xxxxxxxxxxxxxxxx*

Event Code 060A

Explanation

Session services is waiting for a direct search list (DSRLST) response with the SLU destination for an INIT OTHER CD. Parameter *xxx...xxx* is the 8-byte PCID associated with the session.

Event ID:
EIDSIOCD

Event Format:
060A *xxxxxxxxxxxxxxxx*

Event Code 060B

Explanation

Session services is waiting for a DSRLST response to determine the network ID of the DLU. The DSRLST was sent for another session and the same DLU.

Event ID:
EIDSDNTS

Event Format:
060B *xxxxxxxxxxxxxxxx yyyyyyyyyyyyyyyy*

Event Code 060C

Explanation

Session services is waiting to obtain a cryptographic key for the session during CDINIT request or response processing.

Event ID:
EIDSCDCR

Event Format:
060C *xxxxxxxxxxxxxxxx*

Event Code 060D

Explanation

Session services is waiting to obtain a cryptographic key for the session during DSRLST processing.

Event ID:
EIDSDSCR

Event Format:
060D *xxxxxxxxxxxxxxxx*

Event Code 060E

Explanation

Session services is waiting to obtain a cryptographic key for the session during DEQUEUE request processing.

Event ID:
EIDSDQRQ

Event Format:
060E *xxxxxxxxxxxxxxxx*

Event Code 060F

Explanation

Session services is waiting to obtain a cryptographic key for the session during DEQUEUE response processing.

Event ID:
EIDSDQRS

Event Format:
060F *xxxxxxxxxxxxxxxx*

Event Code 0610

Explanation

Session services is waiting for an RTP start event to be completed. Parameter *xx...xxx* is the 8-byte PCID of the session that is waiting for the RTP start event to complete.

Event ID:
EIDRTIDC

Event Format:
0610 RTPS *xxxxxxxx*

Code 0701 (session services LQAB 2 group)

The wait state event code and ID associated with the session services miscellaneous LQAB 2 group and its meaning is as follows:

Event Code 0701

Explanation

Session services is waiting for a session setup attempt to succeed or fail so that the session initiator may be notified. Parameter *xxx...xxx* is an 8-byte hexadecimal procedure correlation ID (PCID). Parameter *yyy...yyy* is the 8-byte name of the SSCP in the OLU direction. Parameter *zzz...zzz* is the 8-byte name of the logical unit.

Event ID:
EIDINTFY

Event Format:
0701 *xxxxxxxxxxxxxxxx yyyyyyyyyyyyyyyy zzzzzzzzzzzzzzzz*

Chapter 7. VTAM abend codes

This chapter contains the abend codes related to VTAM. For more information about system codes, see the system code manual for your operating system.

Abend codes indicate that the control program has determined that a task cannot continue processing reliably. For example, an error might have occurred during the execution of a user application program and been detected by VTAM. In such a case, the task is terminated. A completion code indicates the reason for the termination.

See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for information about the abend procedure and TSO/VTAM abends.

Abend code 0A7

Explanation: During VTAM HALT QUICK, VTAM HALT, VTAM HALT CANCEL, or VTAM abnormal termination processing, VTAM found that no storage was available to schedule a TPEND exit for an access method control block (ACB) opened by a user application program or VTAM subtask.

This abend code is also issued during VTAM HALT CANCEL or VTAM abnormal termination processing if a TPEND exit for an ACB does not exist, the ACB was not valid, or the ACB storage was freed.

System action: The user application is abnormally terminated.

Abend code 0A8

Explanation: VTAM detected an error that occurred during the execution of a user application program. The contents of the two low-order bytes of Register 15 indicate the cause of the error.

Register 15 contents (in hex)
Explanation

2101
A VTAM validity check of the user request parameter list (RPL) failed because the RPL does not have the same protection key as the application program task control block (TCB).

7001
The user's event control block (ECB) is not valid.

7002
A VTAM request for storage failed.

7003
The pointer to the request parameter list (RPL) is not valid.

7004
An ACB OPEN failed due to an access method control block (ACB) address that is not valid.

7005
Storage pointed to by RPLAREA is not valid.

7006
Storage pointed to by RPLAAREA is not valid.

7007
The request parameter list (RPL) is not valid. Unable to find ACB.

7008
RPL6 pointed to by RPLAAREA is not valid.

7009
Node initialization block(s) (NIB) pointed to by the request parameter list (RPL) is not valid.

© Copyright IBM Corp. 2000, 2021

700A
Model terminal support (MTS) data pointed to by node initialization block (NIB) is not valid.

700B
Restore parameter list pointed to by node initialization block (NIB) is not valid.

700C
Application-supplied dial parameters storage pointed to by node initialization block (NIB) is not valid.

700D
Bind area pointed to by node initialization block (NIB) is not valid.

7010
An RPL header that was not valid was encountered.

FC01
Network management interface abend.

FC02
VTAM agent user read queue PAB had a storage failure.

FF01
A session awareness (SAW) data buffer that is not valid was passed to VTAM data space services release routine.

System action: The task abnormally terminates.

Programmer response: This is probably a user error.

- For reason codes 2101, 7001, 7003, 7005, 7006, 7007, 7008, 7009, 700A, 700B, and 700C, verify that the RPL and ECB pointers are correct, and execute the job step again.
- For reason code 7004, verify that the ACB pointer is valid and check the storage to be sure it resides in the application storage protection key.
- For reason code 7002, verify that the operator entered the buffer pool or CSA start options as specified in the start procedures.

  Increase storage as required. For insufficient storage errors, you might want to redefine your buffer pool or CSA limits. If the start option cannot be modified using the MODIFY VTAMOPTS command, you must modify the VTAM start options file (ATCSTR*xx*) and restart VTAM to use the new start option.

  – See the Storage Estimate Worksheets in the z/OS Communications Server: SNA Network Implementation Guide to determine the storage requirements for VTAM.
  – See z/OS Communications Server: SNA Resource Definition Reference for a description of VTAM start options.
  – See z/OS Communications Server: SNA Operation for information about the DISPLAY BFRUSE Command, the DISPLAY STORUSE Command, and the MODIFY VTAMOPTS Command.
  – See z/OS Communications Server: SNA Network Implementation Guide for an explanation and description of buffer pools, and for general information about buffer pool specification and allocation.
  – See z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT for information about analyzing dumps and for information about analyzing storage using the VIT analysis tool if external trace is active.
- For reason code 700D, check the application program.
- For reason code FC01, save the dump for problem determination.
- For reason code FF01:
  – If you have access to IBMLink, search for known problems in this area. If no applicable matches are found, report the problem to IBM by using the electronic technical report (ETR) option on IBMLink.
  – If you do not have access to IBMLink, report the problem to the IBM software support center.

Problem Determination:

- If MSGLEVEL=(1,1) was not specified in the JOB statement, specify it and rerun the job.

- Save the console log from the primary console. For systems with remote consoles, save the remote console log. For systems with multiple-console support (MCS), save a copy of the hard copy log.
- Save the job stream associated with the job.
- Make sure that the failing job step includes the SYSABEND DD statement.
- Save all the associated output.
- Save the program listing associated with the job.
- Save the dump.
- Have the linkage editor/loader map available.

Abend code 0A9

For abend code 0A9, the value in Register 15 indicates whether the VTAM module completes successfully and the cause of the errors if the execution a VTAM module failed.

Explanation: When accompanied by a zero value in Register 15, a VTAM HALT command has been successfully completed. If Register 15 is not zero, an error has occurred during the execution of a VTAM module. The contents of the two low-order bytes of Register 15 indicate the cause of the error.

Register 15 contents (in hex)
Explanation

0000
A VTAM HALT CANCEL command has been successfully completed.

10F1
The ABEND was issued by VTAM retry functional recovery routine (FRR) to pass the original abend to the next recovery routine (if any) associated with the task control block (TCB). See the original abend, which was recorded in SYS1.LOGREC and appears just prior to the supervisor call (SVC) dump that was generated and indicated by reason code 10F1.

6901
Error in CP-CP sessions processing. Missing element on list pointed to by AND_BOTH_CP_STATUS_STORAGE_PTR.

6902
Error in CP-CP sessions processing. Missing element on list pointed to by AND_CW_CP_STATUS_STORAGE_PTR.

6903
Error in CP-CP sessions processing. Missing element on list pointed to by AND_CL_CP_STATUS_STORAGE_PTR.

7002
Storage was not available to drive a user exit.

7005
VTAM was unable to restore its registers from the RPH after a user exit routine returned to VTAM.

7006
CPPROC was unable to obtain adequate storage from the vary work area (VWA).

7007
TPEXIT code or CRA RELSTORE code was entered while the process was holding a PSS lock.

7008
A CPWAIT was attempted with an event ID length greater than EIDMAX.

7009
A message module needs more vary work area (VWA) storage within the component recovery area (CRA) than is currently available.

700F
Encountered a session awareness block (SAB) that was not valid.

7010
A GETRDTE or RDTFIND for a resource failed because the resource definition table entry (RDTE) chain has been corrupted.

7012
A lock's count shows no user is holding the lock, but the lock is held.

7013
Lock hierarchy violation.

7014
TSLINK found the component recovery area (CRA) too small to hold all of the data.

7015
A transmission subsystem control block (TSCB) was encountered that is not valid.

7016
ISTAPCPD detected a work element that was not valid or an overlaid work element.

7017
Resource exhausted condition. For example, an internal table is full.

7018
An attempt to initialize a Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) anchor pool failed.

7019
A RoCE anchor pool entry could not be obtained.

701A
A RoCE anchor pool entry could not be marked active.

701B
An attempt to free a RoCE anchor pool failed.

701C
An attempt to initialize a RoCE shared lock failed.

701D
An attempt to free a RoCE shared lock failed.

701E
PSS found corrupted queue on Very Extended PAB.

701F
SETVRR limit exceeded - Only 4 VRRs allowed.

7071
This error is issued for one of the following reasons:

- A RELSTORE was issued for a previously freed buffer.
- A buffer was overlaid.

7072
A VTFREE was issued for a previously freed area.

7074
A VTFREE was issued for a buffer that is not valid.

7075
A FREEBLK was issued for a previously freed storage area.

7076
C code ran out of ISA storage for autodata.

7077
Storage management header has been overlaid.

7078
The last word in the buffer being RELSTOREd is not BFPPCBA (fence corrupted).

7079
Header in REQSTORE buffer being allocated is not valid (no match on fence word).

707A
A FREESTOR was issued for a previously freed storage area.

707B
ISTORMMG detected an overlaid storage management header.

707C
A FREEBLK was issued for a previously free storage area. It is currently queued and waiting to be freed.

CD01
CDRM error detected.

CF01
An error was found and corrected in a CDRM minor node during CDRM major node deactivation.

FA01
DS process error.

FA02
The DS disk I/O subtask has abended due to insufficient storage. The checkpoint has been disabled.

FA09
Initialization error.

FE02
A pool has been defined by the POOLDEF macro with an unacceptable length or the lengths in a variable-length pool were not defined in ascending order.

FE03
The GETSTOR pool was defined with an unacceptable length or lengths not ascending.

FF02
A FREEBLK macro returned a nonzero return code.

FF03
A utility module detected a function code that is not valid.

FF04
A request, response, or vector was not defined to the RU information table.

FF05
The main entry for the extended router was invoked but processing was already occurring within a CALLSSCP environment.

FF06
No sense code was set, but one should have been.

FF07
The CPCBURC field contained no format, but the response has a format.

FF08
The limit of topology elements (SWBVDCVD) has been exceeded. D3/D4 vectors for elements exceeding limit were not built.

FF09
The VWA area in use is too small to satisfy this request.

FF10
A request was made to queue a response to a process anchor block (PAB).

FF11
A suspend code that is not valid was passed to suspend.

FF12
A SENDER invocation that is not valid was made.

FF13
An unexpected value was received. The value might be valid in another context.

FF14
An unexpected finite state machine (FSM) state was encountered.

FF15
An unexpected field value was encountered for an enumerated type.

FF16
An unexpected control block was received as input.

FF17
A session information block (SIB) or SIB address that is not valid was passed to FREESIB.

FF18
The SENDER buffer area is not large enough.

FF19
The DETERMINER routine returned results that are not valid.

FF20
The BUILD routine returned results that are not valid.

FF22
SRTDEL failed.

FF23
A VR out-of-sequence error has occurred. The ABEND has been initiated by VTAM (no dump) to initiate VR recovery.

FF24
VTAM agent user read queue PAB dispatched with incorrect application work element.

FF25
HPRCTL was issued with the TOKEN option and the value passed was not valid.

FF26
Secondary Access Point (SAP) table overflow.

FF27
A freed TG record is still queued to a topology and routing services (TRS) routing tree.

FF99
Indicates that a FFST probe was tripped. Console messages with prefix EPW will be issued by FFST to provide information about the probe trip. See z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT for a description of FFST probes.

System action: The task that initiated the VTAM request abnormally terminates.

Problem Determination:

- If MSGLEVEL=(1,1) was not specified in the JOB statement, specify it and rerun the job.
- Save the console log from the primary console. For systems with remote consoles, save the remote console log. For systems with multiple-console support (MCS), save a copy of the hard copy log.
- Save the job stream associated with the job.
- Make sure that the failing job step includes the:
  1. SYSABEND DD statement.
  2. SYSUDUMP DD statement.
- Save all the associated output.
- Save the dump.
- Execute the EREP service aid to dump the LOGREC file, and save the resulting output. For MSS, execute the following program to dump the LOGREC file:
  1. Service aid IFCISDA0
  2. Program ISDASDAO with the DETAIL(ALL) parameter
- If Register 15 is 7015, take the following actions to try to determine the cause of the TSCB integrity loss:

1. Save the dump.
2. If VTAM internal trace is running MODE=EXT, save this trace.

   Note: The default trace internal options might not be enough to resolve this problem. All options but LOCK, with a trace table of at least SIZE=200, might be required.

Abend code 0AA

Explanation: An abend condition occurred during execution of VTAM. VTAM functional recovery routines (FRRs) were unable to associate the failure with any particular task control block (TCB) in the address space.

System action: All the tasks in the address space are abnormally terminated.

Problem Determination:

- If MSGLEVEL=(1,1) was not specified in the JOB statement, specify it and rerun the job.
- Save the console log from the primary console. For systems with remote consoles, save the remote console log. In systems with multiple-console support (MCS), save a copy of the hard copy log.
- Make sure that the failing job step includes the SYSABEND DD statement.
- Save all the associated output.
- Save the dump.
- Have the linkage editor/loader map available.

Abend code 0AB

Explanation: An error occurred while TSO/VTAM was in operation and a VTIOC module was executing a VTAM macro. The contents of the two low-order bytes of Register 15 indicate the cause of the error.

This error is usually due to a storage problem with the LPBUF or CRPL buffers.

Register 15 contents (in hex)
Explanation

0101
The terminal-input manager for LU1 (for example, IBM 3767 and IBM 3770 terminals) encountered an unrecoverable error while executing a VTAM macro that uses a request parameter list (RPL).

0102
The terminal-output manager for LU1 (for example, IBM 3767 and IBM 3770 terminals) encountered an unrecoverable error while executing a VTAM macro that uses an RPL.

0103
The terminal-input manager for LU0 and LU2 (for example, IBM 3270 SNA terminals) encountered an unrecoverable error while executing a VTAM macro that uses an RPL.

0104
The terminal-output manager for LU0 and LU2 (for example, IBM 3270 SNA terminals) encountered an unrecoverable error while executing a VTAM macro that uses an RPL.

0105
The VTIOC LOSTERM exit routine encountered an error during execution of a SNA BIND or UNBIND command that used an RPL.

0201
An application ID problem was encountered during execution of a VTAM OPEN macro. The error occurred during initialization of a TSO/VTAM user-address space.

0202
An error occurred during execution of a VTAM OPEN macro. The ERROR field of the ACB indicates the problem. The values that can be set in the ERROR field are listed in “ACB OPEN and CLOSE macroinstruction error fields” on page 147.

0203
An error occurred during execution of a VTAM CLOSE macro. The code in the ERROR field of the ACB is X'42', indicating that the ACB has been closed, but a VTAM error has prevented the successful disconnection of one or more TSO terminals.

0204
During a logon for the TSO application, TSO/VTAM issued a QUERY 3270 data stream to determine the characteristics of the terminal. The response to the query was more than 4096 bytes.

System action: The terminal session in which the error occurred terminates.

Problem Determination:

- Save the console log from the primary console. For systems with remote consoles, save the remote console log. For systems with multiple-console support (MCS), save a copy of the hard copy log.
- Save all the associated output.
- Save the dump.
- Execute the EREP service aid to dump the LOGREC file, and save the resulting output. For MSS, execute the following program to dump the LOGREC file:
  1. Service aid IFCISDA0
  2. Program ISDASDAO with the DETAIL(ALL) parameter
- Have the linkage editor/loader map available.

Abend code 0AC

Explanation: The terminal control address space (TCAS) was unable to continue its normal processing because of an error. The low-order bytes of Register 15 and the TCAS work area (TWAR) field TWARSON both contain the reason code that indicates the cause of the error.

Reason code in hexadecimal
Explanation

00
A STOP command was entered.

04
A START command that is not valid was entered.

10
The TCAS main task was unable to attach the VTAM interface subtask.

14
The TCAS main task was unable to attach the user-interface subtask.

18
The TCAS main task was unable to attach the console-communication subtask.

1C
TCAS was unable to obtain storage for the TCAS table (TCAST) in the common service area (CSA).

20
The TCAS main task abnormally terminated and was unable to recover.

30
The VTAM interface subtask abnormally terminated and was unable to recover.

34
The user-interface subtask abnormally terminated and was unable to recover.

38
The console-communication subtask abnormally terminated and was unable to recover.

System action: TCAS abnormally terminates.

Operator Response: Reply ‘DUMP’ to TCAS termination message IKT012D to obtain a dump.

Problem Determination:

- Save the console log from the primary console. For systems with remote consoles, save the remote console log. For systems with multiple-console support (MCS), save a copy of the hard copy log.
- Save the system output (SYSOUT) associated with the job.
- Save all the associated output.
- Save the dump.
- Print the associated SVC dump data set, using IPCS. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for information about IPCS.

Abend code 0AD

Explanation: An error occurred while TSO/VTAM was in operation and VTIOC queue manager was executing a GETCELL or FREECELL macro. The contents of the two low-order bytes of Register 15 indicate the cause of the error.

Register 15 contents (in hex)
Explanation

0108
The cell address supplied to the FREECELL macro is not valid.

010C
No cell pool existed for the FREECELL request.

0110
A cell pool ID that is not valid was specified for the FREECELL request.

020C
No cell pool existed for the GETCELL request.

0210
A cell pool ID that is not valid was specified for the GETCELL request.

System action: The queue manager abnormally terminates, and the terminal session in which the error occurred terminates.

Problem Determination:

- Save the console log from the primary console. For systems with remote consoles, save the remote console log. In systems with multiple-console support (MCS), save a copy of the hard copy log.
- Save the program listing associated with the job.
- Execute the EREP service aid to dump the LOGREC file, and save the resulting output. For MSS, execute the following program to dump the LOGREC file:
  1. Service aid IFCISDA0
  2. Program ISDASDAO with the DETAIL(ALL) parameter
- Have the linkage editor/loader map available.
- Print the associated SVC dump data set, using IPCS. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for information about IPCS.

Chapter 8. ATM network-generated cause and diagnostic codes

ATM network-generated cause and diagnostic codes are issued in some messages when a request for activation of a native ATM permanent virtual channel (PVC) or a switched virtual channel (SVC) fails. These codes provide information about the cause of a failure detected by the ATM network.

This chapter shows possible codes and their meaning.

Note: The codes included in this topic are those defined by the International Telecommunication Union–Telecommunication Standardization Sector (ITU-T), as specified in the *ATM User-Network Interface Specification, Version 3.1* , published by the ATM Forum. If you cannot find a particular code in this topic, see the following ITU-T recommendations or consult your ATM network provider.

- Q.850, *Usage of Cause and Location in DSS 1 and the SS 7 User Part*
- Q.2610, *Broadband Integrated Services Digital Network (B-ISDN) Usage of Cause and Location in B-ISDN User Part and DSS 2*

VTAM hint: A possible cause of many errors indicated by ATM network-generated cause and diagnostic codes is an incorrectly coded DLCADDR operand on a GROUP definition statement in the XCA major node or on the PATH definition statement in the switched major node. See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

ATM network-generated cause codes

This section describes the cause codes that can be displayed.

Table 16. ATM network-generated cause codes

Decimal code	Hexadecimal code	Meaning	Additional diagnostic information
1	1	Unassigned number **Explanation:** The number requested by the calling user cannot be reached because it is not currently assigned to any user by the network.	See “Diagnostic code for cause codes 1, 2, and 49” on page 324.

© Copyright IBM Corp. 2000, 2021

Table 16. ATM network-generated cause codes (continued)

Decimal code	Hexadecimal code	Meaning	Additional diagnostic information
2	2	No route to specified transit network **Explanation:** The equipment issuing this cause received a request to route the call through a transit network that it does not recognize. The equipment issuing this cause does not recognize the transit network because the network does not exist, or the network exists but does not serve the equipment that is sending this cause. This message is network dependent.	None available
3	3	No route to destination **Explanation:** The called user cannot be reached because the network that serves the called user is inaccessible.	See "Diagnostic code for cause codes 1, 2, and 49" on page 324.
10	A	VPCI/VCI unacceptable	None available
16	10	Normal call clearing **Explanation:** The call is being cleared because one of the users involved in the call has requested that the call be cleared.	None available
17	11	User busy **Explanation:** The called user has indicated an inability to accept another call, although the called user equipment is compatible with the call.	None available
18	12	No user responding **Explanation:** The user did not respond to a call establishment message with a connect indication within the time allocated.	None available
21	15	Call rejected **Explanation:** The called user did not accept this call, although it could have been accepted because the called user was neither busy nor incompatible.	See "Diagnostic code for cause code 21" on page 325.

Table 16. ATM network-generated cause codes (continued)

Decimal code	Hexadecimal code	Meaning	Additional diagnostic information
22	16	Number changed **Explanation:** The called party number indicated by the calling user is no longer assigned.	New destination New destination is formatted as the called party number information element, including the information element identifier. Transit network selection might also be included.
23	17	User rejects CLIR **Explanation:** The user rejects all calls with calling line identification restriction (CLIR).	None available
26	1A	Not-selected user clearing **Explanation:** The user has not been routed the incoming call.	None available
27	1B	Destination out of order **Explanation:** The destination cannot be reached because a signaling message could not be delivered to the called user.	None available
28	1C	Incorrect number format (address incomplete) **Explanation:** The called user cannot be reached because the called party number is not a valid format or is not complete.	None available
30	1E	Response to status inquiry **Explanation:** This value is included in the status message after the prior receipt of a status inquiry message.	None available
31	1F	Normal, unspecified **Explanation:** A normal event occurred and no other cause in the normal event class applies.	None available
35	23	Requested VPCI/VCI not available	None available
36	24	VPCI/VCI assignment failure	None available
37	25	User cell rate not available	None available

Table 16. ATM network-generated cause codes (continued)

Decimal code	Hexadecimal code	Meaning	Additional diagnostic information
38	26	Network out of order **Explanation:** The network is not functioning correctly, and the condition is likely to last a long time. Immediately trying a call again is not likely to be successful.	None available
41	29	Temporary failure **Explanation:** The network is not functioning correctly, but the condition is not likely to last a long time. Another call attempt can be tried almost immediately.	None available
43	2B	Access information discarded **Explanation:** The network could not deliver access information to the called user as requested. Access information includes low-layer compatibility and high-layer information.	See "Information element identifier" on page 326. Multiple information element identifiers might be included.
45	2D	No VPCI/VCI available	None available
47	2F	Resource unavailable, unspecified **Explanation:** A resource unavailable event occurred and no other cause in the resource unavailable class applies.	None available
49	31	Quality of service not available **Explanation:** The requested quality of service cannot be provided.	See "Diagnostic code for cause codes 1, 2, and 49" on page 324.
51	33	User cell rate not available	See "ATM user cell rate subfield identifier" on page 327. Multiple ATM user cell rate subfield identifiers might be included.
57	39	Bearer capability not authorized	None available
58	3A	Bearer capability not presently available **Explanation:** The requested bearer service is implemented by the equipment, but it is not available at this time.	None available

Table 16. ATM network-generated cause codes (continued)

Decimal code	Hexadecimal code	Meaning	Additional diagnostic information
63	3F	Service or option not available, unspecified **Explanation:** A service or option is unavailable and no other cause in the service or option-not-available class applies.	None available
65	41	Bearer capability not implemented **Explanation:** The equipment issuing this cause does not support the requested bearer capability.	None available
73	49	Unsupported combination of traffic parameters	None available
78	4E	AAL parameters cannot be supported	None available
79	4F	Service or option not implemented, unspecified **Explanation:** A service or option is not implemented and no other cause in the service or option-not-implemented class applies.	None available
81	51	Incorrect call reference value **Explanation:** The equipment sending the cause received a message with a call reference that is not currently in use on the user-network interface.	None available
82	52	Identified channel does not exist **Explanation:** The equipment issuing this cause received a request to establish a call that has low-layer compatibility, high-layer compatibility, or other compatibility attributes that it cannot accommodate.	See "Virtual path connection identifier (VPCI) and virtual channel identifier (VCI)" on page 327.
88	58	Incompatible destination **Explanation:** The equipment issuing this cause received a request to establish a call that has low-layer compatibility, high-layer compatibility, or other compatibility attributes that it cannot accommodate.	See "Information element identifier" on page 326. Multiple information element identifiers might be included.
89	59	Incorrect endpoint reference	None available

Table 16. ATM network-generated cause codes (continued)

Decimal code	Hexadecimal code	Meaning	Additional diagnostic information
91	5B	Incorrect transit network selection **Explanation:** An incorrectly formatted transit network identifier was received.	None available
92	5C	Too many pending add party requests	None available
93	5D	AAL parameters cannot be supported	None available
95	5F	Incorrect message, unspecified **Explanation:** A message event occurred and no other cause in the incorrect message class applies.	None available
96	60	Mandatory information element is missing **Explanation:** The equipment sending this cause received a message that is missing an information element required to process the message.	See "Information element identifier" on page 326. Multiple information element identifiers might be included.
97	61	Message type does not exist or is not implemented **Explanation:** The equipment sending this cause received a message that it does not recognize because the message is not defined or it is defined but not implemented by the equipment sending the cause.	See "Message type" on page 328.
99	63	Information element does not exist or is not implemented **Explanation:** The equipment sending this cause received a message that included an information element that is not recognized because the identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the equipment issuing the cause does not require the information element to be present in the message for processing.	See "Information element identifier" on page 326. Multiple information element identifiers might be included.

Table 16. ATM network-generated cause codes (continued)			
Decimal code	**Hexadecimal code**	**Meaning**	**Additional diagnostic information**
100	64	Incorrect information element contents **Explanation:** The equipment sending this cause received an information element that it has implemented, but one or more of the parameters in the information element are coded incorrectly or not implemented.	See "Information element identifier" on page 326. Multiple information element identifiers might be included.
101	65	Message not compatible with call state **Explanation:** A message has been received that is incompatible with the call state.	See "Message type" on page 328.
102	66	Recovery on timer expiration **Explanation:** A procedure has been initiated by the expiration of a time in association with Q.2931 error handling procedures.	See "Timer number" on page 330.
104	68	Incorrect message length	None available
111	6F	Protocol error, unspecified **Explanation:** A protocol error event occurred and no other cause in the protocol error class applies.	None available
121	79	Interworking, unspecified **Explanation:** Interworking occurred with a network that does not provide causes for actions that it takes. The precise cause for a message that is being sent cannot be ascertained.	None available

ATM network-generated coding standard

This section describes the coding standard that can be displayed.

Table 17. ATM network-generated coding standard			
Decimal code	**Hexadecimal code**	**Meaning**	**Additional diagnostic information**
0	0	ITU-TS (CCITT) standardized	None available
3	3	Standard defined for the network (either public or private) present on the network side of the interface.	None available

ATM network-generated cause location

This section describes the cause location that can be displayed.

Table 18. ATM network-generated cause location

Decimal code	Hexadecimal code	Meaning	Additional diagnostic information
0	0	user	None available
1	1	Private network serving the local user	None available
2	2	Public network serving the local user	None available
3	3	Transit network	None available
4	4	Public network serving the remote user	None available
5	5	Private network serving the remote user	None available
7	7	International network	None available
10	A	Network beyond interworking point	None available

ATM network-generated diagnostic codes

This section describes the diagnostic codes that can be displayed.

Diagnostic code for cause codes 1, 2, and 49

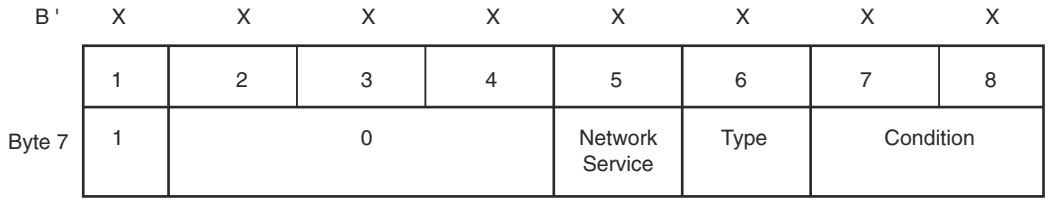

Figure 2. Contents of the diagnostic code for cause codes 1, 2, and 49

Table 19 on page 325 describes the contents of the diagnostic code for cause codes 1, 2, and 49.

Table 19. Diagnostic code for cause codes 1, 2, and 49	
Byte	**Description**
7	**Bit 1 — Extension** **B'1... ....'** Extension **Bits 2–4 — Spare** **B'.0.. ....'** Spare **B'..0. ....'** Spare **B'...0 ....'** Spare **Bit 5 — Network Service** **B'.... 0...'** Provider **B'.... 1...'** User **Bit 6 — Type of Failure** **B'.... .0..'** Normal **B'.... .1..'** Abnormal **Bits 7 and 8 — Condition** **B'.... ..00'** Unknown **B'.... ..01'** Permanent **B'.... ..10'** Transient

Diagnostic code for cause code 21

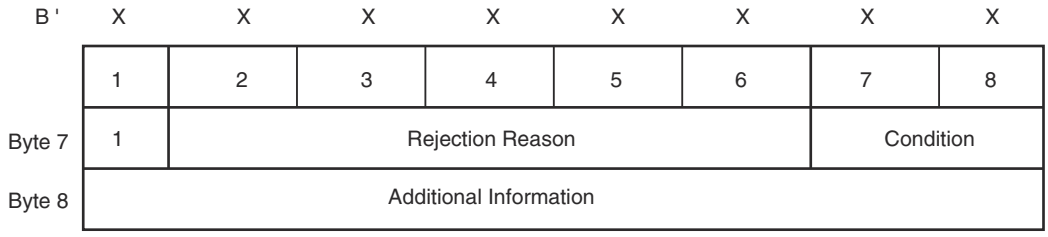

Figure 3. Contents of the diagnostic code for cause codes 21

Table 20 on page 326 describes the contents of the diagnostic code for cause codes 21.

Table 20. Diagnostic code for cause code 21	
Byte	**Description**
7	**Bit 1 — Extension** **B'1... ....'** Extension **Bits 2–6 — Rejection Reason** **B'.000 00..'** User specific **B'.000 01..'** Information element missing **B'.000 10..'** Information element contents are not sufficient **Bits 7 and 8 — Condition** **B'.... ..00'** Unknown **B'.... ..01'** Permanent **B'.... ..10'** Transient
8	If the rejection reason in Byte 7 indicates user specific, Byte 8 is coded to the user specification, subject to the maximum length of the cause information element. If the rejection reason in Byte 7 indicates information element missing or information element contents are not sufficient, byte 8 contains the information element identifier of the missing or insufficient information element.

Information element identifier

VTAM hint: A possible cause of many errors indicated by an ATM network-generated information element identifier cause code is an incorrectly coded DLCADDR operand on a GROUP definition statement in the XCA major node or on the PATH definition statement in the switched major node. See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

Hexadecimal code	Meaning
X'08'	Cause
X'14'	Call state
X'54'	Endpoint reference
X'55'	Endpoint state
X'58'	ATM adaptation layer parameters
X'59'	ATM user cell rate
X'5A'	Connection identifier
X'5C'	Quality of service parameter
X'5D'	Broadband high layer information
X'5E'	Broadband bearer capability

Hexadecimal code	Meaning
X'5F'	Broadband low-layer information
X'60'	Broadband locking shift
X'61'	Broadband non-locking shift
X'62'	Broadband sending complete
X'63'	Broadband repeat indicator
X'6C'	Calling party number
X'6D'	Calling party subaddress
X'70'	Called party number
X'71'	Called party subaddress
X'78'	Transit network selection
X'79'	Restart indicator

ATM user cell rate subfield identifier

VTAM hint: A possible cause of many errors indicated by an ATM network-generated ATM user cell rate subfield identifier cause code is an incorrectly coded DLCADDR operand on a GROUP definition statement in the XCA major node or on the PATH definition statement in the switched major node. See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

Hexadecimal code	Meaning
X'82'	Forward peak cell rate identifier (CLP=0)
X'83'	Backward peak cell rate identifier (CLP=0)
X'84'	Forward peak cell rate identifier (CLP=0+1)
X'85'	Backward peak cell rate identifier (CLP=0+1)
X'88'	Forward sustainable cell rate identifier (CLP=0)
X'89'	Backward sustainable cell rate identifier (CLP=0)
X'90'	Forward sustainable cell rate identifier (CLP=0+1)
X'91'	Backward sustainable cell rate identifier (CLP=0+1)
X'A0'	Forward maximum burst size identifier (CLP=0)
X'A1'	Backward maximum burst size identifier (CLP=0)
X'B0'	Forward maximum burst size identifier (CLP=0+1)
X'B1'	Backward maximum burst size identifier (CLP=0+1)
X'BE'	Best effort indicator
X'BF'	Traffic management options identifier

Virtual path connection identifier (VPCI) and virtual channel identifier (VCI)

VTAM hint: A possible cause of many errors indicated by an ATM network-generated VPCI/VCI cause code is an incorrectly coded DLCADDR operand on a GROUP definition statement in the XCA major node

or on the PATH definition statement in the switched major node. See z/OS Communications Server: SNA Resource Definition Reference for information about how to code the DLCADDR operand on the GROUP definition statement in the XCA major node and for information about how to code the DLCADDR operand on the PATH definition statement in the switched major node.

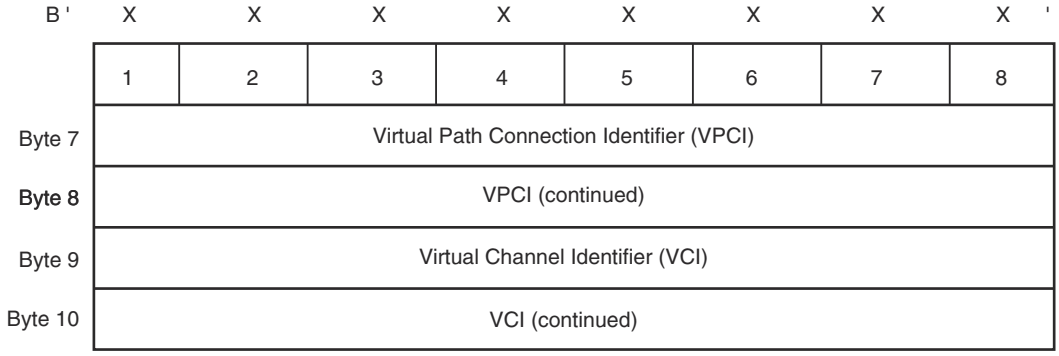

Figure 4. Contents of the VPCI/VCI diagnostic code

Table 21 on page 328 describes the contents of the VPCI/VCI diagnostic code.

Table 21. Virtual path connection identifier and virtual channel identifier

Byte	Description
7	Virtual path connection identifier (VPCI)
8	VPCI (continued)
9	Virtual channel identifier (VCI)
10	VCI (continued)

Message type

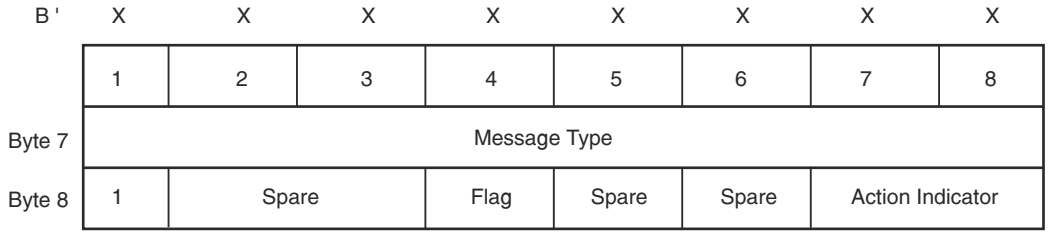

Figure 5. Contents of the message type diagnostic code

Table 22 on page 329 describes the contents of the message type diagnostic code.

Table 22. Message type	
Byte	**Description**
7	**Call Establishment Messages**: **X'02'** CALL PROCEEDING **X'07'** CONNECT **X'0F'** CONNECT ACKNOWLEDGE **X'05'** SETUP **Call Clearing Messages**: **X'4D'** RELEASE **X'5A'** RELEASE COMPLETE **X'46'** RESTART **X'4E'** RESTART ACKNOWLEDGE **Point-to-Multipoint Messages**: **X'80'** ADD PARTY **X'81'** ADD PARTY ACKNOWLEDGE **X'82'** ADD PARTY REJECT **X'83'** DROP PARTY **X'84'** DROP PARTY ACKNOWLEDGE **Miscellaneous Messages**: **X'7D'** STATUS **X'75'** STATUS ENQUIRY

Table 22. Message type (continued)	
Byte	**Description**
8	**Bit 1 — Extension** **B'1... ....'** Extension **Bits 2 and 3 — Spare** **B'.0.. ....'** Spare **B'..0. ....'** Spare **Bit 4 — Flag** **B'...0 ....'** Message instruction field is not significant. Regular error handling procedures apply. Ignore action indicator field. **B'...1 ....'** Follow explicit instructions in the action indicator field that supersedes regular error handling procedures. **Bit 5 — Spare** **B'.... .0..'** Spare **Bit 6 — Spare** **B'.... .0..'** Spare **Bits 7 and 8 — Action Indicator** **B'.... ..00'** Clear call **B'.... ..01'** Discard and ignore **B'.... ..10'** Discard and report status **B'.... ..11'** Reserved

Timer number

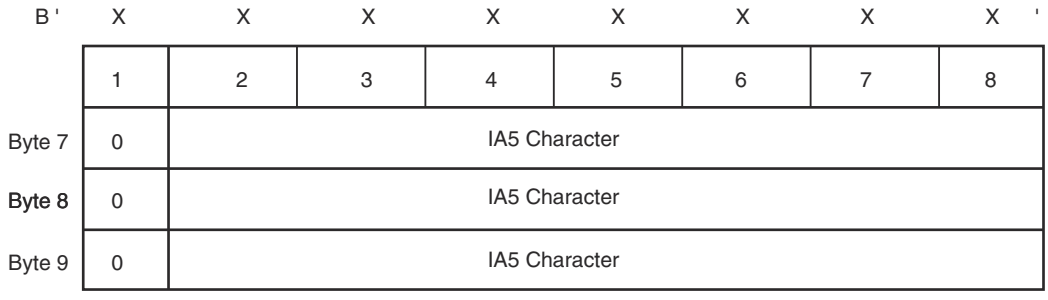

Figure 6. Contents of the timer number diagnostic code

Table 23 on page 331 describes the contents of the timer number diagnostic code.

Table 23. Timer number	
Byte	**Description**
7	**Bit 1 — Spare** **B'0... ....'** Spare **Bits 2–7 — IA5 Character**

Chapter 9. SNA coupling facility user reason codes

This chapter describes the MVS Coupling Facility user reason codes.

Rebuild start reason codes

This section describes the connector specific reason codes for starting a rebuild. These codes will appear in the MVS message IXC526I.

00000108*x* storage shortage

VTAM detected a shortage of either storage entries or data elements in a coupling facility structure. VTAM was unable to adjust the number of entries or elements using the structure alter process, so a rebuild is started to adjust the number of entries or elements.

00000112*x* loss of connectivity

VTAM lost connectivity to a coupling facility structure. Because the sysplex failure management (SFM) policy is not in effect, VTAM is starting a rebuild to attempt to reestablish connectivity.

00000114*x* list number expansion

All list headers in the coupling facility structure are being used. VTAM is starting a rebuild to expand the number of list headers allocated in the structure.

Rebuild stop reason codes

This section describes the connector specific reason codes for stopping a rebuild. These codes will appear in the MVS message IXC527I.

00000100*x* response failure

VTAM was unable to respond to an event during a rebuild. The rebuild is stopped to avoid a hang situation in the rebuild state.

VTAM hint: This is caused by an unexpected return code from the IXLEERSP programming interface that VTAM uses to respond to particular events received from MVS. Attempt the rebuild again. If the rebuild continues to be stopped with this code, contact IBM Service.

00000104*x* local repopulation failure

VTAM was unable to complete repopulating the data in the rebuild structure from the local data.

VTAM hint: This is a result of an unexpected failure during the repopulation phase of the rebuild. Contact IBM Service.

© Copyright IBM Corp. 2000, 2021

Chapter 10. TCP/IP codes

This chapter contains the GDDMXD/MVS, MVP, and SNALU6.2 codes.

GDDMXD/MVS abend codes

This topic contains GDDMXD/MVS abend codes.

102

Severity

Recoverable error.

Explanation

Either of the load modules GDXLIOX0 or GDXADML1 could not be found.

System action

The GDDM application is terminated.

User response

Check that the load library for GDDMXD/MVS is allocated in STEPLIB.

System programmer response

None.

Module

N/A

Destination

N/A

103

Severity

Recoverable error.

Explanation

The X Window System was unable to connect to the workstation at the internet address specified in the *user_id*.XWINDOWS.DISPLAY data set.

System action

The GDDM application is terminated.

© Copyright IBM Corp. 2000, 2021

User response

Correct the address in *user_id*.XWINDOWS.DISPLAY data set, and try again.

System programmer response

None.

Module

GDXLINX0

Destination

gdxlinx0

104

Severity

Recoverable error.

Explanation

The X Window System has detected an error and is unable to continue. This abend is generally preceded by an X Window System message.

System action

The GDDM application is terminated.

User response

Try again. If the error continues to occur, contact the IBM Software Support Center.

System programmer response

None.

Module

GDXLANX0, GDXLDSX0, GDXLINX0, GDXLRDX0

Destination

N/A

105

Severity

Recoverable error.

Explanation

An unexpected condition has occurred. This can be caused by some previous error condition or incomplete program termination.

System action

The GDDM application is terminated.

User response

Issue the TSO LOGON command. If the error persists, contact the IBM Software Support Center.

System programmer response

None.

Module

N/A

Destination

N/A

MVS platform (MVPMAIN) completion codes

This section contains MVPMAIN completion codes

The following return codes are issued from the MVPMAIN module, which is the MVS platform module responsible for establishing the execution environment for many of the tasks started to support TCP/IP services. These return codes or task completion codes appear in the job log for the started task (within message IEF142I). They also appear as part of a task completion message written to the operator console.

1*xx*

Explanation

An attempt to obtain virtual storage for the MVPCOMM (common) table using the GETMAIN macro interface was unsuccessful. The *xx* portion of the completion code is the GETMAIN return code.

System action

The system terminates the task.

Operator response

Tell the system programmer about the error.

System programmer response

Increase the region size in the catalogued procedure used to start the task. If region size is not the problem, gather all available documentation, and report the error to the IBM Software Support Center.

Module

MVPMAIN

Destination

mainline code

200

Explanation

A subtask of MVPMAIN abended.

System action

The system ends the task.

Operator response

Tell the system programmer about the error.

System programmer response

Check the job log to identify the failing task. Use the dump from the abend to determine the cause of the failure in the subtask. See the z/OS MVS Diagnosis: Reference for more information about debugging abends.

Module

MVPMAIN

Destination

mainline code

316

Explanation

An attempt to load the message data set MVPMSGS was unsuccessful.

System action

The system terminates the task.

Operator response

Tell the system programmer about the error.

System programmer response

Check that the identified module resides in a library that is accessible to the MVS platform code. See z/OS Communications Server: IP Configuration Reference for information about required library residence for TCPIP components. If residency requirements are met, gather all available documentation, and report the error to the IBM Software Support Center.

Module

MVPMAIN

Destination

mainline code

516

Explanation

An attempt to load module MVPTASK was unsuccessful. This module is responsible for attaching all subtasks of the MVS platform.

System action

The system terminates the task.

Operator response

Tell the system programmer about the error.

System programmer response

Check that the identified module resides in a library that is accessible to the MVS platform code. See z/OS Communications Server: IP Configuration Reference for information about required library residence for TCPIP components. If residency requirements are met, gather all available documentation, and report the error to the IBM Software Support Center.

Module

MVPMAIN

Destination

mainline code

600

Explanation

Module MVPMAIN could not find the entry for the VMCF subsystem address space during a scan of SSCVT (SubSystems Communications Vector Table).

System action

The system terminates the task.

Operator response

Tell the system programmer about the error.

System programmer response

Verify that the VMCF subsystem is being created and initialized during system initialization. See Step 3: Configure VMCF and TNF in z/OS Communications Server: IP Configuration Guide for more information about starting VMCF and TNF.

Module

MVPMAIN

Destination

mainline code

7*xx*

Explanation

An error occurred attempting to return virtual storage for the MVPCOMM (common) table using the FREEMAIN macro interface. The *xx* portion of the completion code is the FREEMAIN return code. This error occurred during task termination processing.

System action

The system terminates the task.

Operator response

Tell the system programmer about the error.

System programmer response

This error usually occurs because of corruption of the storage used to anchor the MVPCOMM control block. Determine if any previous operator messages were issued that might indicate contributing error conditions within the MVS platform. Gather all available documentation and report the error to the IBM Software Support Center.

Module

MVPMAIN

Destination

mainline code

8*xx*

Explanation

An attempt to obtain virtual storage for I/O completion and attention work areas using the GETMAIN macro interface was unsuccessful. The *xx* portion of the completion code is the GETMAIN return code.

System action

The system terminates the task.

Operator response

Tell the system programmer about the error.

System programmer response

Increase the region size in the catalogued procedure used to start the task. If region size is not the problem, gather all available documentation, and report the error to the IBM Software Support Center.

Module

MVPMAIN

Destination

mainline code

9*xx*

Explanation

An ENQ macro was issued with a resource name of TCPIPSYS.task_name, requesting exclusive use. The ENQ invocation failed, with the *xx* portion of the completion code being the ENQ return code.

System action

The system ends the task.

Operator response

If the error was an unintentional attempt to start a TCPIP task that was already active, then no actions are required. Otherwise, tell the system programmer about the error.

System programmer response

If the error was not because of an unintentional attempt to start a duplicate TCPIP task, examine the task completion code. For information about interpreting the return code, see the z/OS MVS Programming: Assembler Services Reference ABE-HSP. Follow recommended problem resolution procedures indicated by the appropriate MVS diagnostics manual.

Note: The ENQ was issued with the RET=USE parameter.

If problem determination indicates that the MVS platform is in error, gather all available documentation, and report the error to the IBM Software Support Center.

Module

MVPMAIN

Destination

mainline code

MVS platform (MVPXVI) completion codes

This section contains MVPXVI completion codes.

The following return codes are issued from the MVPXVI, which is the module responsible for initializing the address space that provides VMCF/DLC emulation services.

52

Explanation

An attempt to establish the interface to the VMCF subsystem through program calls (PCs) was unsuccessful. Module MVPXGPC returned a nonzero return code from its invocation to create a PC entry table.

System action

The system terminates the VMCF subsystem.

Operator response

Tell the system programmer about the error.

System programmer response

This error usually occurs because of a programming error in generating the macros responsible for defining the PC entry table. Determine if a refresh of module MVPXGPC resolves the problem. Otherwise, report the error to the IBM Software Support Center.

Module

MVPXVI

Destination

mainline code

3016

Explanation

An attempt to load the message data set MVPMSGS was unsuccessful.

System action

The system terminates the VMCF subsystem.

Operator response

Tell the system programmer about the error.

System programmer response

Check that the identified module resides in a library that is accessible to the MVS platform code. For information about the required library residence for TCPIP components, see z/OS Communications Server: IP Configuration Reference. If residency requirements are met, gather all available documentation, and report the error to the IBM Software Support Center.

Module

MVPXVI

Destination

mainline code

4000

Explanation

During VMCF address space initialization, either module MVPXVI was unable to find the entry for the VMCF subsystem address space during a scan of subsystems communications vector table (SSCVT), or the entry was successfully located, but the pointer to the VMCF communications vector table (CVT) contained a value of zero.

System action

The system terminates the VMCF subsystem.

Operator response

Tell the system programmer about the error.

System programmer response

Verify that the VMCF subsystem is being created and initialized during system initialization. See Step 3: Configure VMCF and TNF in z/OS Communications Server: IP Configuration Guide for more information about starting VMCF and TNF.

Module

MVPXVI

Destination

mainline code

5000

Explanation

During VMCF address space initialization, either module MVPXVI was unable to find the entry for the Termination Notification Facility (TNF) subsystem address space during a scan of SSCVT (subsystems communications vector table), or the entry was successfully located, but the pointer to the TNF communications vector table (CVT) contained a value of zero.

System action

The system terminates the VMCF subsystem.

Operator response

Tell the system programmer about the error.

System programmer response

Verify that the VMCF subsystem is being created and initialized during system initialization. See Step 3: Configure VMCF and TNF in z/OS Communications Server: IP Configuration Guide for more information about starting VMCF and TNF.

Module

MVPXVI

Destination

mainline code

70*xx*

Explanation

An error occurred attempting to return virtual storage for the VMCF common tables using the FREEMAIN macro interface. The *xx* portion of the completion code is the FREEMAIN return code. This error occurred during subsystem termination processing.

System action

The system terminates the VMCF subsystem.

Operator response

Tell the system programmer about the error.

System programmer response

This error usually occurs because of corruption of the storage used to anchor the VMCF common control blocks. Determine if any previous operator messages were issued that indicate contributing error conditions within the VMCF subsystem. Gather all available documentation and report the error to the IBM Software Support Center.

Module

MVPXVI

Destination

mainline code

SNALU6.2 abend codes

The following codes are abend codes for SNALU6.2.

1

Explanation

The CANCEL subcommand has been entered from an operator console (using a MODIFY console command).

System programmer response

None.

100

Explanation

An error was encountered during the processing of an DLC interrupt. The reason code contained in Register 15 indicates the exact nature of the error.

Reason
Explanation

1
A non-DLC event was found on the DLC event queue.

2
An unexpected DLC interrupt type was encountered.

System programmer response

Contact the IBM Software Support Center.

200

Explanation

An error was encountered during the processing of a VTAM interrupt. The reason code contained in Register 15 indicates the exact nature of the error.

Reason
Explanation

1
An expected exit type was found in a VTAM event queue element.

2
An unexpected ATTN exit type was encountered.

System programmer response

Contact the IBM Software Support Center.

210

Explanation

A error was detected in one of the internal data structures. The reason code contained in Register 15 indicates the exact nature of the error.

Reason
Explanation

1
The free pool of connection table entries was exhausted; sufficient entries should have been allocated during initialization.

2
An incorrect connection entry address was found in the word immediately preceding the RPL record passed to an allocate request.

3
An incorrect connection entry address was found in the word immediately preceding the RPL record passed to a deallocate request.

4
An incorrect connection entry address was found in the word immediately preceding the RPL record passed to a send request.

5
An incorrect connection entry address was found in the word immediately preceding the RPL record passed to a receive request.

6
The RPL address returned from a VTAM deallocate request does not match either the send or receive RPL address.

7
The VTAM send queue was empty when it was expected to contain an entry.

8
A counter, which contains the number of entries in the VTAM send, contains a negative number.

9
An attempt to terminate a connection with a destination node has failed because of a probable program logic error.

10
An error occurred while adding a connection to the time-out inactivity list; the connection entry address did not reference a valid connection table entry.

11
A connection table entry has been lost from the time-out inactivity list.

12
The RPL address returned from VTAM for a conversation allocation request did not match either the send or receive RPL address.

13
The free pool for the pending message queue was exhausted; sufficient entries should have been allocated during initialization.

System programmer response

Contact the IBM Software Support Center.

220

Explanation

The return codes from a VTAM APPC command indicate that the RPL specified was not valid.

System programmer response

Contact the IBM Software Support Center.

300

Explanation

An error was detected during a GETMAIN macro execution. The reason code contained in register 15 indicates the exact nature of the error.

Reason
Explanation

1
Insufficient storage for subroutine stacks

2
Insufficient storage for major data structures

System programmer response

Increase the value of the REGION parameter for the address space, and restart the address space.

310

Explanation

An unexpected data set identifier was passed to an I/O utility routine.

System programmer response

Contact the IBM Software Support Center.

320

Explanation

An error was detected in the subroutine stack processing logic. The reason code contained in Register 15 indicates the exact nature of the error.

Reason
Explanation

1
Stack Overflow

2
Stack Underflow

3
Stack not empty on exit from program

System programmer response

Contact the IBM Software Support Center.

331

Explanation

An invalid number of arguments was passed to a subroutine in the SNALINK LU6.2 address space.

System programmer response

Contact the IBM Software Support Center.

Chapter 11. SNMP pe_error messages

This chapter contains descriptions of the pe_errors that can appear when the SNMP query engine is decoding the presentation elements from a presentation stream.

Class/ID mismatch in constructor

Explanation

The SNMP query engine was decoding a constructed presentation element, but the presentation element did not have the expected class and ID.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the presentation stream is correct, then the SNMP query engine built the corresponding presentation element incorrectly. Contact the IBM Software Support Center.

Not a constructor form

Explanation

The SNMP query engine expected the presentation element being decoded to be a constructed form, but it was not.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the presentation stream is correct, then the SNMP query engine built the corresponding presentation element incorrectly. Contact the IBM Software Support Center.

Not a primitive form

Explanation

The SNMP query engine expected the presentation element to have a form of primitive. Either the form was not primitive, or the form was primitive but the presentation element had no value associated with it.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the presentation stream is correct, then the SNMP query engine built the corresponding presentation element incorrectly. Contact the IBM Software Support Center.

Out of memory

Explanation

The SNMP query engine could not allocate enough memory to decode the presentation element.

© Copyright IBM Corp. 2000, 2021

User response

Restart the SNMP query engine with a larger region size.

Overflow

Explanation

The length of the value in the presentation element was larger than the length allowed for that data type.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the presentation stream is correct, then the SNMP query engine built the corresponding presentation element incorrectly. Contact the IBM Software Support Center.

Chapter 12. SNMP ps_error messages

This chapter contains descriptions of the ps_errors that can appear when the SNMP query engine is converting a presentation stream into a series of presentation elements.

End of file

Explanation

The SNMP query engine attempted to read the presentation stream, but there is no data to be read.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

End of file reading extended ID

Explanation

The SNMP query engine attempted to read the extended ID in the tag field of the ASN.1 type but could not find the data to read.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

End of file reading extended length

Explanation

The SNMP query engine attempted to read the extended length field of the ASN.1 type but could not find the data to read.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

Indefinite length in primitive form

Explanation

The SNMP query engine attempted to read a primitive ASN.1 type, but the primitive ASN.1 type had an indefinite length field. This is not allowed by SNMP.

© Copyright IBM Corp. 2000, 2021

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

Length Mismatch

Explanation

The SNMP query engine attempted to read a constructed ASN.1 type, but the SNMP query engine found an inconsistency between the length of the data to be read and the actual data read.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

Out of memory

Explanation

The SNMP query engine could not allocate enough memory to process the presentation stream.

User response

Restart the SNMP query engine with a larger region size.

Overflow in ID

Explanation

An overflow occurred reading the extended ID of the tag field of an ASN.1 type.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

Overflow in length

Explanation

The length specified in the tag field of an ASN.1 type is larger the allowed length.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client

or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

XXX

Explanation

The SNMP query engine attempted to read a primitive ASN.1 type, but either the pointer to the presentation stream was null, or the length field of the ASN.1 type was larger than the number of bytes remaining to be read in the presentation stream.

User response

Run traces to determine whether the error is in the incoming presentation stream or in the SNMP query engine translation process. If the presentation stream is in error, contact the support center of the client or agent originating the request. If the SNMP query engine is reading the presentation stream incorrectly, contact the IBM Software Support Center.

Chapter 13. Sockets and sockets extended return codes (ERRNOs)

If the return code is not listed in topic, it is a return code that is received from z/OS UNIX. See the z/OS UNIX System Services Messages and Codes for the z/OS UNIX System Services ERRNOs.

Sockets return codes (ERRNOs)

This section provides the system-wide message numbers and codes set by the system calls. These message numbers and codes are in the TCPERRNO.H include file supplied with TCP/IP Services.

Table 24. Sockets ERRNOs

Error number	Message name	Socket API type	Error description	Programmer's response
1	EAI_NONAME	GETADDRINFO GETNAMEINFO	NODE or HOST cannot be found.	Ensure the NODE or HOST name can be resolved.
1	EDOM	All	Argument too large.	Check parameter values of the function call.
1	EPERM	All	Permission is denied. No owner exists.	Check that TCP/IP is still active; check protocol value of socket () call.
1	EPERM	IOCTL (SIOCGPARTNERINFO)	Both endpoints do not reside in the same security domain.	Check and modify the security domain name for the endpoints. After you correct the security domain name, the application might need to close the connection if the IOCTL is needed.
1	EPERM	IOCTL (SIOCGPARTNERINFO, SIOCSPARTNERINFO)	The security domain name is not defined.	Define the security domain name on both endpoints. After you define the security domain name, the application might need to close the connection if the IOCTL is needed.
1	EPERM	IOCTL (SIOCTTLSCTL)	Denotes one of the following error conditions: • The TTLS_INIT_ CONNECTION option was requested with either TTLS_RESET_ SESSION, TTLS_RESET_ CIPHER, TTLS_RESET_WRITE_CIPHER, TTLS_SEND_SESSION_TICKET, or TTLS_STOP_ CONNECTION • The TTLS_STOP_ CONNECTION option was requested along with TTLS_RESET_ SESSION, TTLS_RESET_ CIPHER, TTLS_RESET_WRITE_CIPHER, or TTLS_SEND_SESSION_TICKET • The TTLS_ALLOW_ HSTIMEOUT option was requested without TTLS_INIT_ CONNECTION • The TTLS_RESET_WRITE_CIPHER option was requested along with TTLS_RESET_SESSION or TTLS_RESET_CIPHER • The TTLS_SEND_SESSION_TICKET option was requested along with TTLS_RESET_SESSION, TTLS_RESET_CIPHER, or TTLS_RESET_WRITE_CIPHER	Request TTLS_RESET_SESSION, TTLS_RESET_CIPHER, TTLS_RESET_WRITE_CIPHER, or TTLS_SEND_SESSION_TICKET only when TTLS_INIT_ CONNECTION and TTLS_STOP_ CONNECTION are not requested. Always request TTLS_INIT_ CONNECTION when TTLS_ALLOW_ HSTIMEOUT is requested. Use seperate SIOCTTLSCTL ioctls to request TTLS_INIT_ CONNECTION and TTLS_STOP_ CONNECTION. Use separate SIOCTTLSCTL ioctls to request TTLS_RESET_WRITE_CIPHER or TTLS_SEND_SESSION_TICKET.
2	EAI_AGAIN	FREEADDRINFO GETADDRINFO GETNAMEINFO	For GETADDRINFO, NODE could not be resolved within the configured time interval. For GETNAMEINFO, HOST could not be resolved within the configured time interval. The Resolver address space has not been started. The request can be retried later.	Ensure the Resolver is active, then retry the request.
2	ENOENT	All	The data set or directory was not found.	Check files used by the function call.
2	ERANGE	All	The result is too large.	Check parameter values of the function call.

© Copyright IBM Corp. 2000, 2021

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
3	EAI_FAIL	FREEADDRINFO GETADDRINFO GETNAMEINFO	This is an unrecoverable error. NODELEN, HOSTLEN, or SERVLEN is incorrect. For FREEADDRINFO, the resolver storage does not exist.	Correct the NODELEN, HOSTLEN, or SERVLEN. Otherwise, call your system administrator.
3	ESRCH	All	The process was not found. A table entry was not located.	Check parameter values and structures pointed to by the function parameters.
4	EAI_OVERFLOW	GETNAMEINFO	The output buffer for the host name or service name was too small.	Increase the size of the buffer to 255 characters, which is the maximum size permitted.
4	EINTR	All	A system call was interrupted.	Check that the socket connection and TCP/IP are still active.
5	EAI_FAMILY	GETADDRINFO GETNAMEINFO	The AF or the FAMILY is incorrect.	Correct the AF or the FAMILY.
5	EIO	All	An I/O error occurred.	Check status and contents of source database if this occurred during a file access.
6	EAI_MEMORY	GETADDRINFO GETNAMEINFO	The resolver cannot obtain storage to process the host name.	Contact your system administrator.
6	ENXIO	All	The device or driver was not found.	Check status of the device attempting to access.
7	E2BIG	All	The argument list is too long.	Check the number of function parameters.
7	EAI_BADFLAGS	GETADDRINFO GETNAMEINFO	FLAGS has an incorrect value.	Correct the FLAGS.
8	EAI_SERVICE	GETADDRINFO	The SERVICE was not recognized for the specified socket type.	Correct the SERVICE.
8	ENOEXEC	All	An EXEC format error occurred.	Check that the target module on an exec call is a valid executable module.
9	EAI_SOCKTYPE	GETADDRINFO	The SOCTYPE was not recognized.	Correct the SOCTYPE.
9	EBADF	All	An incorrect socket descriptor was specified.	Check socket descriptor value. It might be currently not in use or incorrect.
9	EBADF	Givesocket	The socket has already been given. The socket domain is not AF_INET or AF_INET6.	Check the validity of function parameters.
9	EBADF	Select	One of the specified descriptor sets is an incorrect socket descriptor.	Check the validity of function parameters.
9	EBADF	Takesocket	The socket has already been taken.	Check the validity of function parameters.
9	EAI_SOCKTYPE	GETADDRINFO	The SOCTYPE was not recognized.	Correct the SOCTYPE.
10	ECHILD	All	There are no children.	Check if created subtasks still exist.
11	EAGAIN	All	There are no more processes.	Retry the operation. Data or condition might not be available at this time.
11	EAGAIN	All	TCP/IP is not active at the time of the request.	Start TCP/IP, and retry the request.
11	EAGAIN	IOCTL (SIOCGPARTNERINFO)	The IOCTL was issued in no-suspend mode and the SIOCSPARTNERINFO IOCTL has not been issued.	Reissue the IOCTL with a timeout value to set the amount of time to wait while the partner security credentials are being retrieved. **Restriction:** You cannot use a select mask to determine when an IOCTL is complete, because an IOCTL is not affected by whether the socket is running in blocking or nonblocking mode. If the IOCTL times out, reissue the IOCTL to retrieve the partner security credentials.
12	ENOMEM	All	There is not enough storage.	Check the validity of function parameters.
13	EACCES	All	Permission denied, caller not authorized.	Check access authority of file.
13	EACCES	IOCTL (SIOCGPARTNERINFO)	The application is not running in supervisor state, is not APF authorized, or is not permitted to the appropriate SERVAUTH profile.	Allow the application to issue this IOCTL, or provide the user ID with the proper SERVAUTH permission.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
13	EACCES	IOCTL (SIOCTTLSCTL)	The IOCTL is requesting a function that requires that the socket be mapped to policy that specifies ApplicationControlled On.	Check policy and add ApplicationControlled On if the application should be permitted to issue the controlled SIOCTTLSCTL functions.
13	EACCES	Takesocket	The other application (listener) did not give the socket to your application. Permission denied, caller not authorized.	Check access authority of file.
14	EFAULT	All	An incorrect storage address or length was specified.	Check the validity of function parameters.
14	EFAULT	All EZASMI macros when using an asynchronous exit routine.	The exit routine has abnormally ended (ABEND condition).	Correct the error in the routine's code. Add an ESTAE routine to the exit.
14	EFAULT	IOCTL (SIOCSAPPLDATA)	An abend occurred while attempting to copy the SetADcontainer structure from the address provided in the SetAD_ptr field.	Check the validity of function parameters.
15	ENOTBLK	All	A block device is required.	Check device status and characteristics.
16	EBUSY	All	Listen has already been called for this socket. Device or file to be accessed is busy.	Check if the device or file is in use.
17	EEXIST	All	The data set exists.	Remove or rename existing file.
18	EXDEV	All	This is a cross-device link. A link to a file on another file system was attempted.	Check file permissions.
19	ENODEV	All	The specified device does not exist.	Check file name and if it exists.
20	ENOTDIR	All	The specified directory is not a directory.	Use a valid file that is a directory.
21	EISDIR	All	The specified directory is a directory.	Use a valid file that is not a directory.
22	EINVAL	All types	An incorrect argument was specified.	Check the validity of function parameters.
22	EINVAL	Multicast Source filter APIs	Mix of any-source, source-specific or full-state APIs	Specify the correct type of APIs.
22	EINVAL	MCAST_JOIN_GROUP, MCAST_JOIN_SOURCE_ GROUP, MCAST_BLOCK_SOURCE, MCAST_LEAVE_GROUP, MCAST_LEAVE_SOURCE_ GROUP, MCAST_UNBLOCK_ SOURCE, SIOCGMSFILTER, SIOCSMSFILTER	The socket address family or the socket length of the input multicast group or the source IP address is not correct.	Specify the correct value.
22	EINVAL	SIOCSMSFILTER, SIOCSIPMSFILTER	The specified filter mode is not correct.	Specify the correct value.
23	ENFILE	All	Data set table overflow occurred.	Reduce the number of open files.
24	EMFILE	All	The socket descriptor table is full.	Check the maximum sockets specified in MAXDESC().
25	ENOTTY	All	An incorrect device call was specified.	Check specified IOCTL() values.
26	ETXTBSY	All	A text data set is busy.	Check the current use of the file.
27	EFBIG	All	The specified data set is too large.	Check size of accessed dataset.
28	ENOSPC	All	There is no space left on the device.	Increase the size of accessed file.
29	ESPIPE	All	An incorrect seek was attempted.	Check the offset parameter for seek operation.
30	EROFS	All	The data set system is Read only.	Access data set for read only operation.
31	EMLINK	All	There are too many links.	Reduce the number of links to the accessed file.
32	EPIPE	All	The connection is broken. For socket write/send, peer has shut down one or both directions.	Reconnect with the peer.
32	EPIPE	IOCTL (SIOCTTLSCTL requesting TTLS_INIT_ CONNECTION, TTLS_RESET_CIPHER, TTLS_RESET_WRITE_CIPHER, TTLS_SEND_SESSION_TICKET or TTLS_STOP_ CONNECTION)	The TCP connection is not in the established state.	Issue the SIOCTTLSCTL IOCTL when the socket is connected.
33	EDOM	All	The specified argument is too large.	Check and correct function parameters.
34	ERANGE	All	The result is too large.	Check function parameter values.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
35	EWOULDBLOCK	Accept	The socket is in nonblocking mode and connections are not queued. This is not an error condition.	Reissue Accept().
35	EWOULDBLOCK	IOCTL (SIOCTTLSCTL)	The handshake is in progress and the socket is a nonblocking socket.	For a nonblocking socket, you can wait for the handshake to complete by issuing Select or Poll for Socket Writable.
35	EWOULDBLOCK	Read Recvfrom	The socket is in nonblocking mode and read data is not available. This is not an error condition.	Issue a select on the socket to determine when data is available to be read or reissue the Read()/Recvfrom().
35	EWOULDBLOCK	All receive calls (RECV, RECVMSG, RECVFROM, READV, READ), when the socket is set with the SO_RCVTIMEO socket option	The socket is in blocking mode and the receive call has blocked for the time period that was specified in the SO_RCVTIMEO option. No data was received.	The application should reissue the receive call.
35	EWOULDBLOCK	Send Sendto Write	The socket is in nonblocking mode and buffers are not available.	Issue a select on the socket to determine when data is available to be written or reissue the Send(), Sendto(), or Write().
35	EWOULDBLOCK	All send calls (SEND, SENDMSG, SENDTO, WRITEV, WRITE), when the socket is set with the SO_SNDTIMEO socket option	The socket is in blocking mode and the send call has blocked for the time period that was specified in the SO_SNDTIMEO option. No data was sent.	The application should reissue the send call.
36	EINPROGRESS	Connect	The socket is marked nonblocking and the connection cannot be completed immediately. This is not an error condition.	See the Connect() description for possible responses.
36	EINPROGRESS	IOCTL (SIOCGPARTNERINFO)	The IOCTL was issued in no-suspend mode after the SIOCSPARTNERINFO IOCTL was issued, but the partner security credentials are not currently available.	Retry the IOCTL, or issue the IOCTL with a timeout value to set the amount of time to wait while the partner security credentials are being retrieved. **Restriction:** You cannot use a select mask to determine when an IOCTL is complete, because an IOCTL is not affected by whether the socket is running in blocking or nonblocking mode. If the IOCTL times out, reissue the IOCTL to retrieve the partner security credentials.
36	EINPROGRESS	IOCTL (SIOCTTLSCTL requesting TTLS_INIT_ CONNECTION or TTLS_STOP_ CONNECTION)	The handshake is already in progress and the socket is a nonblocking socket.	For a nonblocking socket, you can wait for the handshake to complete by issuing Select or Poll for Socket Writable.
37	EALREADY	Connect	The socket is marked nonblocking and the previous connection has not been completed.	Reissue Connect().
37	EALREADY	IOCTL (SIOCGPARTNERINFO)	The request is already in progress. Only one IOCTL can be outstanding.	Check and modify the socket descriptor, if specified; otherwise, no action is needed.
37	EALREADY	IOCTL (SIOCTTLSCTL requesting TTLS_INIT_ CONNECTION or TTLS_STOP_ CONNECTION)	For TTLS_INIT_ CONNECTION, the socket is already secure. For TTLS_STOP_ CONNECTION, the socket is not secure.	Modify the application so that it issues the SIOCTTLSCTL IOCTL that requests TTLS_INIT_ CONNECTION only when the socket is not already secure and that requests TTLS_STOP_ CONNECTION only when the socket is secure.
37	EALREADY	Maxdesc	A socket has already been created calling Maxdesc() or multiple calls to Maxdesc().	Issue Getablesize() to query it.
37	EALREADY	Setibmopt	A connection already exists to a TCP/IP image. A call to SETIBMOPT (IBMTCP_IMAGE), has already been made.	Call Setibmopt() only once.
38	ENOTSOCK	All	A socket operation was requested on a nonsocket connection. The value for socket descriptor was not valid.	Correct the socket descriptor value and reissue the function call.
39	EDESTADDRREQ	All	A destination address is required.	Fill in the destination field in the correct parameter and reissue the function call.
40	EMSGSIZE	Sendto Sendmsg Send Write for Datagram (UDP) or RAW sockets	The message is too long. It exceeds the IP limit of 64K or the limit set by the setsockopt() call.	Either correct the length parameter, or send the message in smaller pieces.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
41	EPROTOTYPE	All	The specified protocol type is incorrect for this socket.	Correct the protocol type parameter.
41	EPROTOTYPE	bind2addrsel	The referenced socket is not a stream (TCP) or datagram (UDP) socket.	Issue bind2addrsel() on TCP or UDP sockets only.
41	EPROTOTYPE	IOCTL (SIOCGPARTNERINFO, SIOCSAPPLDATA, SIOCSPARTNERINFO, SIOCTTLSCTL)	Socket is not a TCP socket.	Issue the IOCTL on TCP sockets only.
42	ENOPROTOOPT	Getsockopt Setsockopt	The socket option specified is incorrect or the level is not SOL_SOCKET. Either the level or the specified optname is not supported.	Correct the level or optname.
42	ENOPROTOOPT	Getibmsockopt Setibmsockopt	Either the level or the specified optname is not supported.	Correct the level or optname.
43	EPROTONOSUPPORT	Socket	The specified protocol is not supported.	Correct the protocol parameter.
44	ESOCKTNOSUPPORT	All	The specified socket type is not supported.	Correct the socket type parameter.
45	EOPNOTSUPP	Accept Givesocket	The selected socket is not a stream socket.	Use a valid socket.
45	EOPNOTSUPP	bind2addrsel	The referenced socket is not a type that supports the requested function	Use a socket of the correct type.
45	EOPNOTSUPP	Getibmopt Setibmopt	The socket does not support this function call. This command is not supported for this function.	Correct the command parameter. See Getibmopt() for valid commands. Correct by ensuring a Listen() was not issued before the Connect().
45	EOPNOTSUPP	GETSOCKOPT	The specified GETSOCKOPT OPTNAME option is not supported by this socket API.	Correct the GETSOCKOPT OPTNAME option.
45	EOPNOTSUPP	IOCTL	The specified IOCTL command is not supported by this socket API.	Correct the IOCTL COMMAND.
45	EOPNOTSUPP	IOCTL (SIOCSPARTNERINFO)	The request must be issued before the listen call or the connect call.	Check and modify the socket descriptor, or close the connection and reissue the call.
45	EOPNOTSUPP	IOCTL (SIOCTTLSCTL requesting TTLS_INIT_ CONNECTION, TTLS_RESET_ SESSION, TTLS_RESET_ CIPHER, TTLS_RESET_WRITE_CIPHER, TTLS_SEND_SESSION_TICKET, or TTLS_STOP_ CONNECTION)	Mapped policy indicates that AT-TLS is not enabled for the connection.	Modify the policy to enable AT-TLS for the connection.
45	EOPNOTSUPP	Listen	The socket does not support the Listen call.	Change the type on the Socket() call when the socket was created. Listen() supports only a socket type of SOCK_STREAM.
45	EOPNOTSUPP	RECV, RECVFROM, RECVMSG, SEND, SENDTO, SENDMSG	The specified flags are not supported on this socket type or protocol.	Correct the FLAG.
46	EPFNOSUPPORT	All	The specified protocol family is not supported or the specified domain for the client identifier is not AF_INET=2.	Correct the protocol family.
47	EAFNOSUPPORT	bind2addrsel inet6_is_srcaddr	You specified an IP address that is not an AF_INET6 IP address	Correct the IP address. If the IP address is an IPv4 address, you must specify it as an IPv4-mapped IPv6 address.
47	EAFNOSUPPORT	bind2addrsel inet6_is_srcaddr	You attempted an IPv6-only API for a stack that does not support the AF_INET6 domain.	Activate the AF_INET6 stack, and retry the request.
47	EAFNOSUPPORT	Bind Connect Socket	The specified address family is not supported by this protocol family.	For Socket(), set the domain parameter to AF_INET. For Bind() and Connect(), set Sin_Family in the socket address structure to AF_INET.
47	EAFNOSUPPORT	Getclient Givesocket	The socket specified by the socket descriptor parameter was not created in the AF_INET domain.	The Socket() call used to create the socket should be changed to use AF_INET for the domain parameter.
47	EAFNOSUPPORT	IOCTL	You attempted to use an IPv4-only ioctl on an AF_INET6 socket.	Use the correct socket type for the ioctl or use an ioctl that supports AF_INET6 sockets.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
48	EADDRINUSE	Bind, Connect	The address is in a timed wait because a LINGER delay from a previous close or another process is using the address. This error can also occur if the port specified in the bind call has been configured as RESERVED on a port reservation statement in the TCP/IP profile.	To reuse the same address, use Setsockopt() with SO_REUSEADDR. See the section about Setsockopt() in z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference for more information. Otherwise, use a different address or port in the socket address structure.
48	EADDRINUSE	IP_ADD_MEMBERSHIP, IP_ADD_SOURCE_ MEMBERSHIP, IPV6_JOIN_GROUP, MCAST_JOIN_GROUP, MCAST_JOIN_SOURCE_ GROUP	The specified multicast address and interface address (or interface index) pair is already in use.	Correct the specified multicast address, interface address, or interface index.
49	EADDRNOTAVAIL	Bind	The specified address is incorrect for this host.	Correct the function address parameter.
49	EADDRNOTAVAIL	Connect	The calling host cannot reach the specified destination.	Correct the function address parameter.
49	EADDRNOTAVAIL	bind2addrsel	For the specified destination address, there is no source address that the application can bind to. Possible reasons can be one of the following situations: • The socket is a stream socket, but the specified destination address is a multicast address. • No ephemeral ports are available to assign to the socket.	Correct the function address parameter or issue the request when ephemeral ports are available.
49	EADDRNOTAVAIL	inet6_is_srcaddr	The address specified is not correct for one of these reasons: • The address is not an address on this node. • The address was not active at the time of the request. • The scope ID specified for a link-local IPV6 address is incorrect.	Correct or activate the address
49	EADDRNOTAVAIL	IP_BLOCK_SOURCE, IP_ADD_SOURCE_ MEMBERSHIP, MCAST_BLOCK_SOURCE, MCAST_JOIN_SOURCE_ GROUP	A duplicate source IP address is specified on the multicast group and interface pair.	Correct the specified source IP address.
49	EADDRNOTAVAIL	IP_UNBLOCK_SOURCE, IP_DROP_SOURCE_ MEMBERSHIP, MCAST_UNBLOCK_ SOURCE, MCAST_LEAVE_SOURCE_ GROUP	A previously blocked source multicast group cannot be found.	Correct the specified address.
49	EADDRNOTAVAIL	Multicast APIs	The specified multicast address, interface address, or interface index is not correct.	Correct the specified address.
50	ENETDOWN	All	The network is down.	Retry when the connection path is up.
51	ENETUNREACH	Connect	The network cannot be reached.	Ensure that the target application is active.
52	ENETRESET	All	The network dropped a connection on a reset.	Reestablish the connection between the applications.
53	ECONNABORTED	All	The software caused a connection abend.	Reestablish the connection between the applications.
54	ECONNRESET	All	The connection to the destination host is not available.	N/A
54	ECONNRESET	Send Write	The connection to the destination host is not available.	The socket is closing. Issue Send() or Write() before closing the socket.
55	ENOBUFS	All	No buffer space is available.	Check the application for massive storage allocation call.
55	ENOBUFS	Accept	Not enough buffer space is available to create the new socket.	Call your system administrator.
55	ENOBUFS	IOCTL (SIOCGPARTNERINFO)	The buffer size provided is too small.	Create a larger input buffer based on the value returned in the PI_Buflen field.
55	ENOBUFS	IOCTL (SIOCSAPPLDATA)	There is no storage available to store the associated data.	Call your system administrator.
55	ENOBUFS	IOCTL (SIOCTTLSCTL TTLS_Version1 requesting TTLS_RETURN_ CERTIFICATE or TTLS_Version2 query)	The buffer size provided is too small.	For TTLS_Version1 use the returned certificate length to allocate a larger buffer and reissue IOCTL with the larger buffer.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
55	ENOBUFS	IP_BLOCK_SOURCE, IP_ADD_SOURCE_ MEMBERSHIP, MCAST_BLOCK_SOURCE, MCAST_JOIN_SOURCE_ GROUP, SIOCSIPMSFILTER, SIOCSMSFILTER, setipv4sourcefilter, setsourcefilter	A maximum of 64 source filters can be specified per multicast address, interface address pair.	Remove unneeded source IP addresses and reissue the command.
55	ENOBUFS	Send Sendto Write	Not enough buffer space is available to send the new message.	Call your system administrator.
55	ENOBUFS	Takesocket	Not enough buffer space is available to create the new socket.	Call your system administrator.
56	EISCONN	Connect	The socket is already connected.	Correct the socket descriptor on Connect() or do not issue a Connect() twice for the socket.
57	ENOTCONN	All	The socket is not connected.	Connect the socket before communicating.
57	ENOTCONN	IOCTL (SIOCGPARTNERINFO)	The requested socket is not connected.	Check and modify the socket descriptor, or reissue the IOCTL after the connect call from the client side or after the accept call from the server side.
57	ENOTCONN	IOCTL (SIOCTTLSCTL)	The socket is not connected.	Issue the SIOCTTLSCTL IOCTL only after the socket is connected.
58	ESHUTDOWN	All	A Send cannot be processed after socket shutdown.	Issue read/receive before shutting down the read side of the socket.
59	ETOOMANYREFS	All	There are too many references. A splice cannot be completed.	Call your system administrator.
59	ETOOMANYREFS	IP_ADD_MEMBERSHIP, IP_ADD_SOURCE_ MEMBERSHIP, MCAST_JOIN_GROUP, MCAST_JOIN_SOURCE_ GROUP, IPV6_JOIN_GROUP	A maximum of 20 multicast groups per single UDP socket or a maximum of 256 multicast groups per single RAW socket can be specified.	Remove unneeded multicast groups and reissue the command.
60	ETIMEDOUT	Connect	The connection timed out before it was completed.	Ensure the server application is available.
61	ECONNREFUSED	Connect	The requested connection was refused.	Ensure server application is available and at specified port.
62	ELOOP	All	There are too many symbolic loop levels.	Reduce symbolic links to specified file.
63	ENAMETOOLONG	All	The file name is too long.	Reduce size of specified file name.
64	EHOSTDOWN	All	The host is down.	Restart specified host.
65	EHOSTUNREACH	All	There is no route to the host.	Set up network path to specified host and verify that host name is valid.
66	ENOTEMPTY	All	The directory is not empty.	Clear out specified directory and reissue call.
67	EPROCLIM	All	There are too many processes in the system.	Decrease the number of processes or increase the process limit.
68	EUSERS	All	There are too many users on the system.	Decrease the number of users or increase the user limit.
69	EDQUOT	All	The disk quota has been exceeded.	Call your system administrator.
70	ESTALE	All	An old NFS** data set handle was found.	Call your system administrator.
71	EREMOTE	All	There are too many levels of remote in the path.	Call your system administrator.
72	ENOSTR	All	The device is not a stream device.	Call your system administrator.
73	ETIME	All	The timer has expired.	Increase timer values or reissue function.
73	ETIME	IOCTL (SIOCGPARTNERINFO)	The wait time for the request has expired, possibly as the result of network problems.	Retry the request. **Restriction:** You cannot use a select mask to determine when an IOCTL is complete, because an IOCTL is not affected by whether the socket is running in blocking or nonblocking mode. If the IOCTL times out, reissue the IOCTL to retrieve the partner security credentials.
74	ENOSR	All	There are no more stream resources.	Call your system administrator.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
75	ENOMSG	All	There is no message of the desired type.	Call your system administrator.
76	EBADMSG	All	The system cannot read the message.	Verify that z/OS Communications Server installation was successful and that message files were properly loaded.
77	EIDRM	All	The identifier has been removed.	Call your system administrator.
78	EDEADLK	All	A deadlock condition has occurred.	Call your system administrator.
78	EDEADLK	Select Selectex	None of the sockets in the socket descriptor sets are either AF_INET or AF_IUCV sockets and there is no timeout value or no ECB specified. The select/selectex would never complete.	Correct the socket descriptor sets so that an AF_INET or AF_IUCV socket is specified. A timeout or ECB value can also be added to avoid the select/selectex from waiting indefinitely.
79	ENOLCK	All	No record locks are available.	Call your system administrator.
80	ENONET	All	The requested machine is not on the network.	Call your system administrator.
81	ERREMOTE	All	The object is remote.	Call your system administrator.
82	ENOLINK	All	The link has been severed.	Release the sockets and reinitialize the client-server connection.
83	EADV	All	An ADVERTISE error has occurred.	Call your system administrator.
84	ESRMNT	All	An SRMOUNT error has occurred.	Call your system administrator.
85	ECOMM	All	A communication error has occurred on a Send call.	Call your system administrator.
86	EPROTO	All	A protocol error has occurred.	Call your system administrator.
86	EPROTO	IOCTL (SIOCTTLSCTL requesting TTLS_RESET_SESSION, TTLS_RESET_CIPHER, TTLS_RESET_WRITE_CIPHER, TTLS_SEND_SESSION_TICKET, TTLS_STOP_CONNECTION, or TTLS_ALLOW_HSTIMEOUT)	One of the following errors occurred: • A TTLS_INIT_CONNECTION request was not received for the connection. • TTLS_STOP_CONNECTION was requested on a connection that has outstanding application data. For unread application data, the errno junior is JrTTLSStopReadDataPending. For unwritten application data, the errno junior is JrTTLSStopWriteDataPending. • TTLS_RESET_CIPHER or TTLS_STOP_ CIPHER was requested on a connection that is secured using SSL version 2. • TTLS_RESET_WRITE_CIPHER or TTLS_SEND_SESSION_TICKET was requested on a connection that is secured using a protocol version less than TLS version 1.3. • TTLS_ALLOW_HSTIMEOUT was requested but the policy has the HandshakeRole value `client` or the HandshakeTimeout value is 0. • TTLS_SEND_SESSION_TICKET was requested but the policy has the HandshakeRole value client or GSK_SESSION_TICKET_SERVER_ENABLE value Off or the GSK_SESSION_TICKET_SERVER_COUNT value is not 0.	• Request TTLS_INIT_CONNECTION before requesting TTLS_RESET_SESSION, TTLS_RESET_CIPHER, TTLS_RESET_WRITE_CIPHER, or TTLS_SEND_SESSION_TICKET. • Request TTLS_STOP_CONNECTION after all application data is cleared from the connection. For JrTTLSStopReadDataPending, read all available application data. For JrTTLSStopWriteDataPending, wait for all the outstanding application data to be written. • Request TTLS_RESET_CIPHER or TTLS_STOP_CONNECTION only on connections secured using SSL version 3 or TLS version 1.0 or higher. • Request TTLS_RESET_WRITE_CIPHER or TTLS_SEND_SESSION_TICKET only on connections secured using TLS version 1.3 or higher. • Request TTLS_ALLOW_HSTIMEOUT only when the security type is TTLS_SEC_SERVER or higher and the HandshakeTimeout value is not 0. • Request TTLS_SEND_SESSION_TICKET only when the security type is TTLS_SEC_SERVER or higher and when GSK_SESSION_TICKET_SERVER_ENABLE is On and GSK_SESSION_TICKET_SERVER_COUNT is 0.
87	EMULTIHOP	All	A multi-hop address link was attempted.	Call your system administrator.
88	EDOTDOT	All	A cross-mount point was detected. This is not an error.	Call your system administrator.
89	EREMCHG	All	The remote address has changed.	Call your system administrator.
90	ECONNCLOSED	All	The connection was closed by a peer.	Check that the peer is running.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
113	EBADF	All	Socket descriptor is not in correct range. The maximum number of socket descriptors is set by MAXDESC(). The default range is 0–49.	Reissue function with corrected socket descriptor.
113	EBADF	Bind socket	The socket descriptor is already being used.	Correct the socket descriptor.
113	EBADF	Givesocket	The socket has already been given. The socket domain is not AF_INET.	Correct the socket descriptor.
113	EBADF	Select	One of the specified descriptor sets is an incorrect socket descriptor.	Correct the socket descriptor. Set on Select() or Selectex().
113	EBADF	Takesocket	The socket has already been taken.	Correct the socket descriptor.
113	EBADF	Accept	A Listen() has not been issued before the Accept().	Issue Listen() before Accept().
121	EINVAL	All	An incorrect argument was specified.	Check and correct all function parameters.
121	EINVAL	IOCTL (SIOCSAPPLDATA)	The input parameter is not a correctly formatted SetApplData structure. • The SetAD_eye1 value is not valid. • The SetAD_ver value is not valid. • The storage pointed to by SetAD_ptr does not contain a correctly formatted SetADcontainer structure. • The SetAD_eye2 value is not valid. • The SetAD_len value contains an incorrect length for the SetAD_ver version of the SetADcontainer structure.	Check and correct all function parameters.
121	EINVAL	inet6_is_srcaddr	• One or more invalid IPV6_ADDR_ PREFERENCES flags were specified • A scope ID was omitted for a link local IP address • A scope ID was specified for an IP address that is not link-local • The socket address length was not valid	Correct the function parameters
122	ECLOSED			
126	ENMELONG			
134	ENOSYS	IOCTL	The function is not implemented	Either configure the system to support the **ioctl** command or remove the **ioctl** command from your program.
134	ENOSYS	IOCTL - siocgifnameindex	The TCP/IP stack processing the siocgifnameindex IOCTL is configured as a pure IPv4 TCP/IP stack. Additionally, UNIX System Services is configured to process as INET.	Either configure the system to support the **ioctl** command or remove the **ioctl** command from your program.
136	ENOTEMPT			
145	E2BIG	All	The argument list is too long.	Eliminate excessive number of arguments.
156	EMVSINITIAL	All	Process initialization error. This indicates an z/OS UNIX process initialization failure. This is usually an indication that a proper OMVS RACF segment is not defined for the user ID associated with application. The RACF OMVS segment might not be defined or might contain errors such as an improper HOME() directory specification.	Attempt to initialize again. After ensuring that an OMVS Segment is defined, if the errno is still returned, call your MVS system programmer to have IBM service contacted.
157	EMISSED			
157	EMVSERR		An MVS environmental or internal error occurred.	

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
1002	EIBMSOCKOUTOFRANGE	Socket, Accept, Takesocket	A new socket cannot be created because the MAXSOC value, which is specified on the INITAPI call, has been reached.	Take either one of the following actions: • Verify whether all open sockets are intended to be in use. • Increase the MAXSOC value to a value that is appropriate for the current workload. If the default value is currently being used, you might be required to add the INITAPI call.
1003	EIBMSOCKINUSE	Socket	A socket number assigned by the client interface code is already in use.	Use a different socket descriptor.
1004	EIBMIUCVERR	All	The request failed because of an IUCV error. This error is generated by the client stub code.	Ensure IUCV/VMCF is functional.
1008	EIBMCONFLICT	All	This request conflicts with a request already queued on the same socket.	Cancel the existing call or wait for its completion before reissuing this call.
1009	EIBMCANCELLED	All	The request was canceled by the CANCEL call.	Informational, no action needed.
1011	EIBMBADTCPNAME	All	A TCP/IP name that is not valid was detected.	Correct the name specified in the IBM_TCPIMAGE structure.
1011	EIBMBADTCPNAME	Setibmopt	A TCP/IP name that is not valid was detected.	Correct the name specified in the IBM_TCPIMAGE structure.
1011	EIBMBADTCPNAME	INITAPI	A TCP/IP name that is not valid was detected.	Correct the name specified on the IDENT option TCPNAME field.
1012	EIBMBADREQUESTCODE	All	A request code that is not valid was detected.	Contact your system administrator.
1013	EIBMBADCONNECTIONSTATE	All	A connection token that is not valid was detected; bad state.	Verify TCP/IP is active.
1014	EIBMUNAUTHORIZEDCALLER	All	An unauthorized caller specified an authorized keyword.	Ensure user ID has authority for the specified operation.
1015	EIBMBADCONNECTIONMATCH	All	A connection token that is not valid was detected. There is no such connection.	Verify TCP/IP is active.
1016	EIBMTCPABEND	All	An abend occurred when TCP/IP was processing this request.	Verify that TCP/IP has restarted.
1023	EIBMTERMERROR	All	Encountered a terminating error while processing.	Call your system administrator.
1026	EIBMINVDELETE	All	Delete requestor did not create the connection.	Delete the request from the process that created it.
1027	EIBMINVSOCKET	All	A connection token that is not valid was detected. No such socket exists.	Call your system programmer.
1028	EIBMINVTCPCONNECTION	All	Connection terminated by TCP/IP. The token was invalidated by TCP/IP.	Reestablish the connection to TCP/IP.
1032	EIBMCALLINPROGRESS	All	Another call was already in progress.	Reissue after previous call has completed.
1036	EIBMNOACTIVETCP	All	TCP/IP is not installed or not active.	Correct TCP/IP name used.
1036	EIBMNOACTIVETCP	Select	EIBMNOACTIVETCP	Ensure TCP/IP is active.
1036	EIBMNOACTIVETCP	Getibmopt	No TCP/IP image was found.	Ensure TCP/IP is active.
1037	EIBMINVTSRBUSERDATA	All	The request control block contained data that is not valid.	Call your system programmer.
1038	EIBMINVUSERDATA	All	The request control block contained user data that is not valid.	Check your function parameters and call your system programmer.
1040	EIBMSELECTEXPOST	SELECTEX	SELECTEX passed an ECB that was already posted.	Check whether the user's ECB was already posted.
1112	ECANCEL			
1162	ENOPARTNERINFO	IOCTL (SIOCGPARTNERINFO)	The partner resides in a TCP/IP stack running a release that is earlier than V1R12, or the partner is not in the same sysplex.	Ensure that both endpoints reside in TCP/IP stacks that are running V1R12 or any later release, or check and modify the socket descriptor. If the partner is not in the same sysplex, security credentials will not be returned.
2001	EINVALIDRXSOCKETCALL	REXX	A syntax error occurred in the RXSOCKET parameter list.	Correct the parameter list passed to the REXX socket call.

Table 24. Sockets ERRNOs (continued)

Error number	Message name	Socket API type	Error description	Programmer's response
2002	ECONSOLEINTERRUPT	REXX	A console interrupt occurred.	Retry the task.
2003	ESUBTASKINVALID	REXX	The subtask ID is incorrect.	Correct the subtask ID on the INITIALIZE call.
2004	ESUBTASKALREADYACTIVE	REXX	The subtask is already active.	Issue the INITIALIZE call only once in your program.
2005	ESUBTASKNOTACTIVE	REXX	The subtask is not active.	Issue the INITIALIZE call before any other socket call.
2006	ESOCKETNOTALLOCATED	REXX	The specified socket or needed control block could not be allocated.	Increase the user storage allocation for this job.
2007	EMAXSOCKETSREACHED	REXX	The maximum number of sockets has been reached.	Increase the number of allocate sockets, or decrease the number of sockets used by your program.
2009	ESOCKETNOTDEFINED	REXX	The socket is not defined.	Issue the SOCKET call before the call that fails.
2011	EDOMAINSERVERFAILURE	REXX	A Domain Name Server failure occurred.	Call your MVS system programmer.
2012	EINVALIDNAME	REXX	An incorrect *name* was received from the TCP/IP server.	Call your MVS system programmer.
2013	EINVALIDCLIENTID	REXX	An incorrect *clientid* was received from the TCP/IP server.	Call your MVS system programmer.
2014	ENIVALIDFILENAME	REXX	An error occurred during NUCEXT processing.	Specify the correct translation table file name, or verify that the translation table is valid.
2016	EHOSTNOTFOUND	REXX	The host is not found.	Call your MVS system programmer.
2017	EIPADDRNOTFOUND	REXX	Address not found.	Call your MVS system programmer.
2019	ENORECOVERY	REXX	A non-recoverable failure occurred during the Resolver's processing of the GETHOSTBYADDR or GETHOSTBYNAME call.	Contact the IBM support center.
2020	EINVALIDCOMBINATION	REXX	An invalid combination of IPV6_ADDR_PREFERENCES flags was received from the caller.	Correct the specified flags
2021	EOPTNAMEMISMATCH	REXX	The caller specified an OPTNAME that is invalid for the LEVEL that it specified.	Correct either the OPTNAME or the LEVEL.
2022	EFLAGSMISMATCH	REXX	The caller issued a GETADDRINFO with conflicting FLAGS and EFLAGS parameters: either AI_EXT_FLAGS was specified with a null EFLAGS, or AI_EXT_FLAGS was not specified but EFLAGS was not null.	Correct either the FLAGS parameter or the EFLAGS parameter. A non-null EFLAGS should be specified if and only if AI_EXT_FLAGS is specified in the FLAGS.
2051	EFORMATERROR	REXX	The name server was unable to interpret the query	Contact the IBM support center.
3412	ENODATA		Message does not exist.	
3416	ELINKED		Stream is linked.	
3419	ERECURSE		Recursive attempt rejected.	
3420	EASYNC		Asynchronous I/O scheduled. This is a normal, internal event that is NOT returned to the user.	
3448	EUNATCH		The protocol required to support the specified address family is not available.	
3464	ETERM		Operation terminated.	
3474	EUNKNOWN		Unknown system state.	
3495	EBADOBJ		You attempted to reference an object that does not exist.	
3513	EOUTOFSTATE		Protocol engine has received a command that is not acceptable in its current state.	

Sockets extended ERRNOs

Table 25. Sockets extended ERRNOs

Error code	Problem description	System action	Programmer's response
10100	An ESTAE macro did not complete normally.	End the call.	Call your MVS system programmer.
10101	A STORAGE OBTAIN failed.	End the call.	Increase MVS storage in the application's address space.
10108	The first call issued was not a valid first call.	End the call.	Almost all sockets programs that are written in COBOL, PL/I, or assembler language must issue the INITAPI call before they issue other sockets calls.
10110	LOAD of EZBSOH03 (alias EZASOH03) failed.	End the call.	Call the IBM Software Support Center.
10154	Errors were found in the parameter list for an IOCTL call.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the IOCTL call. You might have incorrect sequencing of socket calls.
10155	The length parameter for an IOCTL call is less than or equal to 0.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the IOCTL call. You might have incorrect sequencing of socket calls.
10156	The length parameter for an IOCTL call is 3200 (32 x 100).	Disable the subtask for interrupts. Return an error code to the caller.	Correct the IOCTL call. You might have incorrect sequencing of socket calls.
10159	A 0 or negative data length was specified for a READ or READV call.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the length in the READ call.
10161	The REQARG parameter in the IOCTL parameter list is 0.	End the call.	Correct the program.
10163	A 0 or negative data length was found for a RECV, RECVFROM, or RECVMSG call.	Disable the subtask for interrupts. Sever the DLC path. Return an error code to the caller.	Correct the data length.
10167	The descriptor set size for a SELECT or SELECTEX call is less than or equal to 0.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the SELECT or SELECTEX call. You might have incorrect sequencing of socket calls.

Table 25. Sockets extended ERRNOs (continued)

Error code	Problem description	System action	Programmer's response
10168	The descriptor set size *in bytes* for a SELECT or SELECTEX call is greater than 8192. A number greater than the maximum number of allowed sockets (65534 is the maximum) has been specified.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the descriptor set size.
10170	A 0 or negative data length was found for a SEND or SENDMSG call.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the data length in the SEND call.
10174	A 0 or negative data length was found for a SENDTO call.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the data length in the SENDTO call.
10178	The SETSOCKOPT option length is less than the minimum length.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the OPTLEN parameter.
10179	The SETSOCKOPT option length is greater than the maximum length.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the OPTLEN parameter.
10184	A data length of 0 was specified for a WRITE call.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the data length in the WRITE call.
10186	A negative data length was specified for a WRITE or WRITEV call.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the data length in the WRITE call.
10190	The GETHOSTNAME option length is not in the range of 1–255.	Disable the subtask for interrupts. Return an error code to the caller.	Correct the length parameter.
10193	The SETSOCKOPT or GETSOCKOPT option length is shorter than the minimum length or longer than the maximum length.	End the call.	Correct the length parameter.
10197	The application issued an INITAPI call after the connection was already established.	Bypass the call.	Correct the logic that produces the INITAPI call that is not valid.

Table 25. Sockets extended ERRNOs (continued)

Error code	Problem description	System action	Programmer's response
10198	The maximum number of sockets specified for an INITAPI exceeds 65535.	Return to the user.	Correct the INITAPI call.
10200	The first call issued was not a valid first call.	End the call.	Almost all sockets programs that are written in COBOL, PL/I, or assembler language must issue the INITAPI call before they issue other sockets calls.
10202	The RETARG parameter in the IOCTL call is 0.	End the call.	Correct the parameter list. You might have incorrect sequencing of socket calls.
10203	The requested socket number is a negative value.	End the call.	Correct the requested socket number.
10205	The requested socket number is a duplicate.	End the call.	Correct the requested socket number.
10208	The NAMELEN parameter for a GETHOSTBYNAME call was not specified.	End the call.	Correct the NAMELEN parameter. You might have incorrect sequencing of socket calls.
10209	The NAME parameter on a GETHOSTBYNAME call was not specified.	End the call.	Correct the NAME parameter. You might have incorrect sequencing of socket calls.
10210	The HOSTENT parameter on a GETHOSTBYNAME or GETHOSTBYADDR call was not specified.	End the call.	Correct the HOSTENT parameter. You might have incorrect sequencing of socket calls.
10211	The HOSTADDR parameter on a GETHOSTBYNAME or GETHOSTBYADDR call is incorrect.	End the call.	Correct the HOSTADDR parameter. You might have incorrect sequencing of socket calls.
10212	The resolver program failed to load correctly for a GETHOSTBYNAME or GETHOSTBYADDR call.	End the call.	Check the JOBLIB, STEPLIB, and linklib datasets and rerun the program.
10213	Not enough storage is available to allocate the HOSTENT structure.	End the call.	Increase the user storage allocation for this job.
10214	The HOSTENT structure was not returned by the resolver program.	End the call.	Ensure that the domain name server is available. This can be a nonerror condition indicating that the name or address specified in a GETHOSTBYADDR or GETHOSTBYNAME call could not be matched.
10215	The APITYPE parameter on an INITAPI call instruction was not 2 or 3.	End the call.	Correct the APITYPE parameter.

Table 25. Sockets extended ERRNOs (continued)

Error code	Problem description	System action	Programmer's response
10218	The application programming interface (API) cannot locate the specified TCP/IP.	End the call.	Ensure that an API that supports the performance improvements related to CPU conservation is installed on the system and verify that a valid TCP/IP name was specified on the INITAPI call. This error call might also mean that EZASOKIN could not be loaded.
10219	The NS parameter is greater than the maximum socket for this connection.	End the call.	Correct the NS parameter on the ACCEPT, SOCKET or TAKESOCKET call.
10221	The AF parameter of a SOCKET call is not AF_INET.	End the call.	Set the AF parameter equal to AF_INET.
10222	The SOCTYPE parameter of a SOCKET call must be stream, datagram, or raw (1, 2, or 3).	End the call.	Correct the SOCTYPE parameter.
10223	No ASYNC parameter specified for INITAPI with APITYPE=3 call.	End the call.	Add the ASYNC parameter to the INITAPI call.
10224	The IOVCNT parameter is less than or equal to 0, for a READV, RECVMSG, SENDMSG, or WRITEV call.	End the call.	Correct the IOVCNT parameter.
10225	The IOVCNT parameter is greater than 120, for a READV, RECVMSG, SENDMSG, or WRITEV call.	End the call.	Correct the IOVCNT parameter.
10226	Not valid COMMAND parameter specified for a GETIBMOPT call.	End the call.	Correct the COMMAND parameter of the GETIBMOPT call.
10229	A call was issued on an APITYPE=3 connection without an ECB or REQAREA parameter.	End the call.	Add an ECB or REQAREA parameter to the call.
10300	Termination is in progress for either the CICS transaction or the socket interface.	End the call.	None.
10330	A SELECT call was issued without a MAXSOC value and a TIMEOUT parameter.	End the call.	Correct the call by adding a TIMEOUT parameter.
10331	A call that is not valid was issued while in SRB mode.	End the call.	Get out of SRB mode and reissue the call.
10332	A SELECT call is invoked with a MAXSOC value greater than that which was returned in the INITAPI function (MAXSNO field).	End the call.	Correct the MAXSOC parameter and reissue the call.

Table 25. Sockets extended ERRNOs (continued)

Error code	Problem description	System action	Programmer's response
10334	An error was detected in creating the data areas required to process the socket call.	End the call.	Call the IBM Software Support Center.
10335	An INITAPI or first call was issued by using a TIE that another task used.	End the call.	Change the application to allocate a new TIE or to ensure that a TERMAPI is done before the TIE is reused.
10999	An abend has occurred in the subtask.	Write message EZY1282E to the system console. End the subtask and post the TRUE ECB.	If the call is correct, call your system programmer.
20000	An unknown function code was found in the call.	End the call.	Correct the SOC-FUNCTION parameter.
20001	The call passed an incorrect number of parameters.	End the call.	Correct the parameter list.
20002	The user ID associated with the program linking EZACIC25 does not have the proper authority to execute a CICS EXTRACT EXIT.	End the call.	Start the CICS socket interface before executing this call.
20003	The CICS socket interface is not in operation.	End the call.	Contact the CICS system programmer. Ensure that the user ID being used is permitted to have at least UPDATE access to the EXITPROGRAM resource.
20004	The CICS socket TRUE failed to suspend the task.	End the call.	Call the IBM Software Support Center.
20005	The socket task was purged by CICS while the task was being suspended by the CICS socket TRUE.	End the call.	None.

Chapter 14. TCP/IP abend 3C5 reason codes

001: Bad Load

Explanation

Issued when the routine that is to run under the newly attached task cannot be found.

Module

MVPATT

002: UCB DEQ Failed

Explanation

Issued when the DEQ processing in MVPCLOSE fails with a nonzero return code. Note the resource name that is used is TCPIP.DEV, where is the device number being closed.

Module

MVPCLOSE

003: MVPDG7C Logic error 1

Explanation

Issued by MVPDG7C when an LDSF Present command is issued for a nonexistent LU session.

Module

MVPDG7C

004: MVPDG7C Logic error 2

Explanation

Issued by MVPDG7C when an LDSF Break command is issued for a nonexistent LU session.

Module

MVPDG7C

005: MVPIOINT Circular Q

Explanation

Issued by MVPIOINT when it detects that the TCPIP engine's interrupt queues have been corrupted.

© Copyright IBM Corp. 2000, 2021

Module

MVPIOINT

006: Operator Forced Dump

Explanation

A MODIFY (F) TCPIP,DUMP command was issued from the MVS console.

Module

MVPOCM

007: Get of TNF area failed

Explanation

While attempting to set up a new TNF manager, storage could not be obtained for a TNF manager queue element.

Module

MVPTADD

008: Zero ptr

Explanation

MVPTDEL is attempting to delete a TNF manager for a TNF client address space, and the TNF manager cannot be found.

Module

MVPTDEL

009: Cannot locate TNF SSCT

Explanation

While initializing the TNF address space, an attempt was made to locate the SSCT entry, set up for the TNF subsystem by MVS. It wasn't found.

Note: This should never happen and probably indicates an MVS problem.

Module

MVPTNF

010: Raclow allocate failed

Explanation

MVPUTIL failed when trying to obtain storage for the below-the-line work area needed by RACF.

Module

MVPUTIL

011: Raclow free failed

Explanation

MVPUTIL failed while trying to free the below-the-line RACF work area.

Module

MVPUTIL

012: GARB routine allocation failure

Explanation

MVPUTIL failed while trying to obtain either an I/O interrupt block or an external interrupt block.

Module

MVPUTIL (via MVPGARB macro)

013: VTWK Free error

Explanation

Failure while trying to free a VTRQ queue element.

Module

MVPVTWK

015: Zero token invalid bug

Explanation

While attempting to queue work to the VTAM application task, MVPVTWK detected a VTRQ with a token value of 0.

Module

MVPVTWK (via MVPQTOVT)

016: Unqueue - entry not found

Explanation

MVPXINT tried to take a VMCF interrupt off of an interrupt queue, but the interrupt was not on the queue.

Module

MVPXINT (via MVPXUQ)

017: Message complete not done here

Explanation

Processing detected a message-complete interrupt being queued by IUCV that is not supported in the IUCV implementation. This should not happen and is probably a programming error.

Module

MVPXIUC

018: Bug - wrong type to Q_IUCV_Int

Explanation

Processing tried to queue an invalid interrupt to an IUCV client that is not allowed. This should not happen and is probably a programming error.

Module

MVPXIUC

019: Count going negative

Explanation

The number of interrupts processed by IUCV for a client is greater than the number of interrupts scheduled for that client.

Module

MVPXIUC

020: Bad interrupt type being Queued

Explanation

An interrupt type that is not valid is being queued to a client.

Module

MVPXIUC

021: Caught local lock held in xiuc

Explanation

The VMCF CML lock is held invalidly by the IUCV process.

Module

MVPXIUC

022: Logic error in DoQr MVPXIUC

Explanation

Processing detected an interrupt type that is not valid (not quiesce or resume) passed to the quiesce/resume routine. This should not happen and is probably a programming error.

Module

MVPXIUC

023: GARB routine allocation failure

Explanation

MVPXIUC could not obtain an IUCV_QD block to contain interrupt information.

Module

MVPXIUC (via MVPGARB)

024: Lock not held error

Explanation

The VMCF CML lock was detected as not being held.

Module

MVPXIUT

025: Count going negative

Explanation

The number of interrupts processed by IUCV for a client is greater than the number of interrupts scheduled for that client.

Module

MVPXIUT

026: Internal error in path counting

Explanation

MVPXIUT detected that there are no available paths to which to connect.

Module

MVPXIUT

027: GARB routine allocation failure

Explanation

MVPXIUC could not obtain an IUCV_path block to contain path data.

Module

MVPXIUT (via MVPGARB)

028: Unqueue - entry not found

Explanation

While trying to free an IUCV_QD element, the element could not be found on the interrupt queue.

Module

MVPXIUT (MVPXUQ)

031: Wrong ASCB

Explanation

MVPXTNF is passed a pointer to an ASCB when the failing ASCB goes through termination processing. The TNF entry for the address space contains an ASCB pointer. If these two do not match, an error is detected.

Module

MVPXTNF

032: Caught Local lock held in xtnf

Explanation

MVPXTNF was detected holding the TNF CML lock in error.

Module

MVPXTNF

033: Unqueue - entry not found

Explanation

While trying to take a VMCF interrupt off a client's interrupt queue, the interrupt element was not found.

Module

MVPXUNT (via MVPXUQ)

034: Alloc user data failed

Explanation

MVPXUT could not obtain storage for a user-data entry.

Module

MVPXUT

035: Alloc SRBS failed

Explanation

MVPXUT could not obtain storage for the VMCF/IUCV communications SRBs.

Module

MVPXUT

036: Freemain of SRB failed

Explanation

MVPXUT could not free storage for the VMCF/IUCV communications SRBs.

Module

MVPXUT

037: Getlock for 0 asid

Explanation

A GET for ASID 0's user lock was attempted.

Module

MVPXUT (via MVPXGFL)

038: Local lock not held error

Explanation

A GET of a user lock was attempted, but the VMCF local lock was already held.

Module

MVPXUT (via MVPXGFL)

039: Local lock held

Explanation

The VMCF CML lock is held, but at least one user lock is not held.

Module

MVPXUT (via MVPXGFL)

040: Local lock should be held

Explanation

At least one user lock is held, but the VMCF CML lock is not held.

Module

MVPXUT (via MVPXGFL)

041: Too many locks held

Explanation

Only 4 locks can be held. This request was for a fifth lock.

Module

MVPXUT (via MVPXGFL)

042: User lock already held excl

Explanation

A caller of MVPXUT attempted to upgrade ownership of a user lock to exclusive, but the user already holds the lock exclusive.

Module

MVPXUT (via MVPXGFL)

043: Two user locks in read only

Explanation

A user of MVPXUT that holds a user lock in read-only mode attempted to upgrade the lock to exclusive, but another user lock is held read by the same user. A user lock can be held exclusive only if no other user locks are currently held.

Module

MVPXUT (via MVPXGFL)

044: Upgrade lock by wrong TCB

Explanation

A user attempted to upgrade a user lock to exclusive, but the user is not the one who holds the lock shared.

Module

MVPXUT (via MVPXGFL)

045: User lock not held excl

Explanation

A user attempted to downgrade a user lock from exclusive to shared, but the user does not own the lock exclusive.

Module

MVPXUT (via MVPXGFL)

046: Already holding user lock

Explanation

A user attempted to obtain a user lock that the user already holds. This can happen if a VMCF or IUCV user attempts to send data to himself or herself.

Module

MVPXUT (via MVPXGFL)

047: User lock is not held excl

Explanation

A user attempted to downgrade a user lock from exclusive to shared, but the user does not own the lock exclusive.

Module

MVPXUT (via MVPXGFL)

048: More than two user locks error

Explanation

A user attempted to obtain a third user lock. Only two user locks can be held by the same process at one time.

Module

MVPXUT (via MVPXGFL)

049: holding other user lock exclusively

Explanation

A user attempted to obtain another user's user lock exclusive, but the attempter's own lock is held shared. No lock can be obtained exclusive if more than one user lock is held shared.

Module

MVPXUT (via MVPXGFL)

050: Already held the local lock

Explanation

A user who is attempting to obtain a lock already holds the VMCF CML lock.

Module

MVPXUT (via MVPXGFL)

051: Must hold user lock first

Explanation

A user must hold the user lock before any other lock can be obtained.

Module

MVPXUT (via MVPXGFL)

052: Path lock already held exclusive

Explanation

A user attempted to obtain the path lock exclusive, but it is already held exclusive by another user.

Module

MVPXUT (via MVPXGFL)

053: Already holding path lock

Explanation

A user attempted to obtain the path lock shared, but it is already held shared by another user.

Module

MVPXUT (via MVPXGFL)

054: Lock already held

Explanation

A user attempted to obtain a lock that the user already owns.

Module

MVPXUT (via MVPXGFL)

055: Another subordinate lock held

Explanation

A user requested a subordinate lock, but the user already holds a different one. Only one subordinate lock can be held by one process at one time.

Module

MVPXUT (via MVPXGFL)

056: Freelock for 0 asid

Explanation

A FREE for ASID 0's user lock was attempted.

Module

MVPXUT (via MVPXGFL)

057: Freeing not-held lock

Explanation

A user attempted to free a lock that wasn't owned by the user.

Module

MVPXUT (via MVPXGFL)

058: Subordinate not free

Explanation

A user attempted to free a user lock, but a subordinate lock is still held. Subordinate locks must be freed before any user locks.

Module

MVPXUT (via MVPXGFL)

059: Local lock was not held

Explanation

The VMCF local lock was not held when a free request was processed.

Module

MVPXUT (via MVPXGFL)

060: Caught local lock held in xvmc

Explanation

The VMCF address space CML lock was held in error.

Module

MVPXVMC

061: GARB routine allocation failure

Explanation

A failure occurred while attempting to obtain either a VMCF interrupt block or an intermediate data move buffer.

Module

MVPXVMC (via MVPGARB)

062: Unqueue - entry not found

Explanation

When attempting to remove a VMCF interrupt from a user's interrupt queue, the interrupt element was not found.

Module

MVPXVMC (via MVPXUQ)

063: YSRB Freemain of SRB failed

Explanation

An SRB arrived for a VMCF or IUCV client that has been terminated. The FREEMAIN for the SRB failed.

Module

MVPYSRB

101: Interrupt when INT_GETN. AddUserNote rc not zero.

Explanation

After call to ADDUSERNOTE, PASCROUT was not zero.

Module

IUCVFORC

102: Interrupt when INT_PECB. Circular buffer wrapped.

Explanation

All the space in the circular interrupt buffer has been exhausted.

Module

IUCVFORC

103: In SQLSUBx-TASK. "TODO" not FETCH a row -or- CLOSE DOWN

Explanation

The TODO task must be either fetch a row or close down.

Module

MVPSQL

104: In PUTVTAM. New VTAM PUT addr equals VTAM GET addr.

Explanation

All the space in the circular buffer has been exhausted.

Module

SNALINK

105: In IUCVRUPT. New IUCV PUT addr equals IUCV GET addr.

Explanation

All the space in the circular buffer has been exhausted.

Module

SNALINK

106: Usage error

Explanation

SNALINK entered with a missing parameter. See EZA5775I in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

107: Session Type

Explanation

The session type was coded but invalid. See EZA5842E in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

108: Max RU size

Explanation

The MAX RU size specified is invalid. See EZA5776E in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

109: Storage for path index table

Explanation

There is not enough free storage in the region to satisfy the get main request. See EZA5777E in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

110: IUTIL Init Error

Explanation

There was an error when trying to initialize the IUTIL interface. See EZA5778E in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

111: Missing CONNBLOK

Explanation

There was an error when trying to referrence the session control block. See EZA5809E in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

112: OPENACB failure

Explanation

There was an error when trying to open the ACB with VTAM. See EZA5779E in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

113: SETLOGON failure

Explanation

There was an error when trying to issue the SETLOGON VTAM API call. See EZA5837E in z/OS Communications Server: IP Messages Volume 1 (EZA) for more information.

Module

SNALINK

502: UNITCHEC Freemain error

Explanation

In checking unit name, after linking to IEFEB4UV, the UCB_List was FREEMAINED. FREEMAIN return code was not zero.

Module

MVDYNALL

503: TAPECHEC FREEMAIN ERROR

Explanation

In checking tape name, after linking to IEFEB4UV, the UCB_List was FREEMAINED. FREEMAIN return code was not zero.

Module

MVDYNALL

504: DYNALLOC (SVC 99) failure

Explanation

Invalid text unit error in Dynamic Unallocate parameter list.

Module

MVDYNUN

505: CCALL: Data copy allocate failure

Explanation

GETMAIN failed for the allocated area.

Module

MVPCCALL

506: GARB routine allocate failure

Explanation

GETMAIN failed for the GARB macro (MVPGARB).

Module

MVPCCALL

507: Unexpected GTTERM Return Code

Explanation

In Issue Diagnostic, the GTTERM return code was not zero or eight.

Module

MVPCDODG (ISSUEDIA)

508: Unexpected STFSMODE Return Code

Explanation

The STFSMODE Return Code was not zero.

Module

MVPCDODG (ISSUEDIA)

509: Unexpected TPG Return Code

Explanation

TSO PUT GET return code was not zero.

Module

MVPCDODG (ISSUEDIA)

510: Unexpected Return Code from TGET after TPG

Explanation

TSO TGET Return Code after TPG was not zero.

Module

MVPCDODG (ISSUEDIA)

511: Invalid device for Diagnose 8C

Explanation

In Issue Diagnostic, the second GTTERM return code was eight.

Module

MVPCDODG (ISSUEDIA)

512: Unexpected GTTERM Return Code in Diagnose 8

Explanation

Issue Diagnostic, the 2nd GTTERM return code was not zero or eight.

Module

MVPCDODG (ISSUEDIA)

513: Invalid virtual device number

Explanation

RXF was not a -1 nor a Console_address.

Module

MVPCDODG (ISSUEDIA)

514: Unexpected Diagnose Request

Explanation

The diagnostic request was not DIAGCP, DIAGDEVT or DIAGDEVD.

Module

MVPCDODG (ISSUEDIA)

515: Invalid WSF Data

Explanation

Q_Reply was not a '81'X.

Module

MVPCDODG (ISSUEDIA)

516: Invalid Query Data

Explanation

Querry_Buffer(1:1) was not a X'88'.

Module

MVPCDODG (ISSUEDIA)

517: Unexpected STFSMODE Return Code

Explanation

STFSMODE Return Code was not a zero for special reshow key.

Module

MVPCDODG (DODIAG58)

518: Bad STTMPMD Return Code

Explanation

STTMPMD Return Code was not a zero for PA1.

Module

MVPCDODG (DODIAG58)

519: Bad STTMPMD Return Code

Explanation

STTMPMD Return Code was not a zero when not for PA1.

Module

MVPCDODG (DODIAG58)

520: Unexpected TPUT Return Code

Explanation

TPUT return code was not zero or twenty for CC_Write_Buffer.

Module

MVPCDODG (DODIAG58)

521: Unexpected TGET Return Code

Explanation

TGET return code was not 0, 4, 12, 24 or 28 for CC_Read_Buffer.

Module

MVPCDODG (DODIAG58)

522: Unexpected TGET Return Code

Explanation

TGET return code was not 0, 12, 20, 24 or 28 for Data_Address.

Module

MVPCDODG (DODIAG58)

523: Unexpected TPG Return Code for read buffer

Explanation

PUT/GET return code was not zero or twenty for CC_Write_Buffer.

Module

MVPCDODG (DODIAG58)

524: Unexpected TGET Return Code

Explanation

TGET return code was not 0, 12, 20, 24 or 28 for Data_Address.

Module

MVPCDODG (DODIAG58)

525: Unexpected Diagnose 58 OpCode

Explanation

Diagnois Op_Code was not '29'X or '2A'.

Module

MVPCDODG (DODIAG58)

526: Error allocating write buffer

Explanation

GETMAIN return code was not zero for CC_Write_Buffer.

Module

MVPCDODG (FSIOBEGR)

527: Error allocating read buffer

Explanation

GETMAIN return code was not zero for CC_Read_Buffer.

Module

MVPCDODG (FSIOBEGR)

528: Unexpected STFSMODE Return Code

Explanation

STFSMODE (for OFF) Return Code was not zero.

Module

MVPCDODG (FSIOENDR)

529: Error freeing write buffer

Explanation

FREEMAIN return code was not zero for CC_Write_Buffer.

Module

MVPCDODG (FSIOENDR)

530: Error freeing read buffer

Explanation

FREEMAIN return code was not zero for CC_Read_Buffer.

Module

MVPCDODG (FSIOENDR)

531: Bad STTMPMD Return Code

Explanation

STTMPMD Return Code was not a zero (Reset Display Terminal Manager).

Module

MVPCDODG (FSIOENDR)

532: Unexpected STFSMODE Return Code

Explanation

STFSMODE (for ON) Return Code was not zero.

Module

MVPCDODG (CONWAIT)

533: MVSCLOSE DCB=0

Explanation

CPlist.DCBptr = 0.d

Module

MVPCFIO (MVSCLOSE)

534: MVSPOSIT zero DCBptr

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (MVSPOSIT)

535: BFREAD DCB=0

Explanation

Plist.DCBptr = 0.

Module

MVPCFIO (BFREAD)

536: SLOWSFRE DCB=0

Explanation

Plist.DCBptr = 0.

Module

MVPCFIO (SLOWSFRE)

537: BFWRITE DCB=0

Explanation

Plist.DCBptr = 0.

Module

MVPCFIO (BFWRITE)

538: SFWRITE DCB=0

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (SFWRITE)

539: Null=2

Explanation

If DelimPtr+1 => EndPtr Then there is no room for LF.

Module

MVPCFIO (SFWRITE)

540: Null=1

Explanation

DelimPtr = 0. No Delimeter found.

Module

MVPCFIO (SFWRITE)

541: WRITEBLOck DCB=0

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (WRITEBLO)

542: WRITEBLOck DCB=0

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (WRITEWBL)

543: BLOKREAD DCB=0

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (BLOKREAD)

544: BLOKWRIT DCB=0

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (BLOKWRIT)

545: BLOKINFO DCB=0

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (BLOKINFO)

546: MVSAPPEN DCB=0

Explanation

Plist.DCBptr = 0 at entry.

Module

MVPCFIO (MVSAPPEN)

547: MVPCFIO (MVSMEMLI)

Explanation

MemList bad state. MemList did not return: 1) a fully qualified name, 2) just a member name, or 3) all but prefix.

Module

MVPCFIO

548: DSLIS Free=1

Explanation

FREEMAIN return code was not zero for WorkArea.

Module

MVPCFIO (MVSDSLIS)

549: Bad Locate parms

Explanation

List Cataloged Data Sets (SVC 26) return code was '20'X.

Module

MVPCFIO (MVSDSLIS)

550: DISLIS Free=2

Explanation

FREEMAIN return code was not zero for WorkArea in FreeArea.

Module

MVPCFIO (MVSDSLIS)

551: Bad return code from PUTGET

Explanation

PUTGET for IO parameter list return code not 0, 8, 12, 28 or 32.

Module

MVPCPASS (PASCPASM, PASCPASU)

552: Unexpected TGET Return Code

Explanation

TGET return code was not 0, 4, 12, 24 or 28 for CC_Read_Buffer.

Module

MVPCSEMA

553: Bad RC from STIMERM SET

Explanation

STIMER issued for .5 seconds. Return code not zero.

Module

MVPCSEMA

554: Bad Return Code from IKJEFTSR

Explanation

IKJEFTSR return code 16. One of first six parm addressess is invalid for MVPCTSO.

Module

MVPCTSO (CALLTSO)

555: Bad Return Code from IKJEFTSR

Explanation

IKJEFTSR return code 20. You must analyze the reason code as well.

Module

MVPCTSO (CALLTSO)

556: CXSEM: Data copy free failure

Explanation

FREEMAIN return code was not zero for Complete_Entry.Parm.

Module

MVPCXSEM (ASMWAIT)

557: This return code should not occur.

Explanation

These entries in MVPDODG should never be called. The five entries call a subroutine for MVPDUMP.

Module

MVPDODG (DoDiag58, FsIoEndR, ConWait, DoSioWat and FsIoBegR)

558: GETJOBID ZERO DCBPTR

Explanation

CPlist.DCBptr = 0 at entry.

Module

MVPJES (GETJOBID)

559: Unrecognized Dsorg

Explanation

Dsorg is not PS, PO, DA, IS, VS nor an alias.

Module

MVSTATE (GETSTATE)

560: Incorrect DSCB obtained

Explanation

Module

MVSTATE (GETSTATE)

561: Obtain error

Explanation

Module

MVSTATE (GETSTATE)

Chapter 15. TCP/IP abend 422 reason codes

Abend code 422 is a general-use abend code. It provides an abend that will not be delivered to the target task if the task is already in recovery processing.

This abend might be retryable or non-retryable, depending on the reason code.

The abend 422 reason codes are in the format xxxxyyzz where:

xxxx
The first halfword is for internal use only.

yy
The third byte contains a component identifier. The value 04 is the identifier for Communications Server.

zz
Unique reason code within the component.

The following list contains the reason codes for abend 422.

04FD

Explanation

The target task has a TCP/IP request in progress and is being abended due to TCP/IP abnormal termination initiated by Sysplex Autonomics.

04FE

Explanation

The target task has a TCP/IP request in progress and is being abended due to TCP/IP abnormal termination.

04FF

Explanation

The target task has a TCP/IP request in progress and is being abended due to TCP/IP normal termination.

© Copyright IBM Corp. 2000, 2021

Chapter 16. TCP/IP abend 4C5 reason codes

The abend 4C5 reason codes are in the format xxxxyyyy where:

xxxx
The first halfword is for internal use only.

yyyy
The second halfword contains a unique TCP/IP reason code for abend 4C5.

Tip: If the SBLSCLI0 library is included in the SYSPROC or SYSEXEC search order for a TSO session, use the ERRNO A xxxxyyyy command to interpret these values.

03FE: TcpTerminatedFail

Explanation

This unit of work was running in TCP/IP when TCP/IP was terminated for a failure. This goes with the 422 abend.

03FF: TcpTerminatedNorm

Explanation

This unit of work was running in TCP/IP when TCP/IP was terminated normally. This goes with the 422 abend.

0401: TcpBadEntryCode

Explanation

Bad Entry code to module.

0402: TcpUnexpectedErr

Explanation

Unexpected error.

0403: TcpInBadStack

Explanation

Stack Overflow Error.

0404: TcpLostOMPROUTE

Explanation

TCP stack detected loss of connectivity to OMPROUTE.

© Copyright IBM Corp. 2000, 2021

0405: TcpSysplexUnresponsive

Explanation

The XCF Monitor has determined that the TCP sysplex function is unresponsive.

04C1: TcpINEcode

Explanation

Bad Entry code to module.

04C2: TcpINDspservC

Explanation

Bad RC from DSPSERV Create.

04C3: TcpINAleservA

Explanation

Bad RC from ALESERV Add.

04C4: TcpINAleservE

Explanation

Bad RC from ALESERV Extract.

04C5: TcpINAleservD

Explanation

Bad RC from ALESERV Delete.

04C6: TcpINDspservD

Explanation

Bad RC from DSPSERV Delete.

04C7: TcpINTcbToken

Explanation

Bad RC from TCBTOKEN macro.

04C8: TcpINLxres

Explanation

Bad RC from LXRES macro.

04C9: TcpINAxset

Explanation

Bad RC from AXSET macro.

04CA: TcpINEtcre

Explanation

Bad RC from ETCRE macro.

04CB: TcpINEtcon

Explanation

Bad RC from ETCON macro.

04CC: TcpINEstae

Explanation

Bad RC from ESTAE macro.

04CD: TcpINBadVSMLoc

Explanation

Bad RC from VSM Locate macro.

04CE: TcpINBadLoad

Explanation

Bad RC from LOAD or NUCLKUP macros.

04CF: TcpINEtdes

Explanation

Bad RC from ETDES macro.

04D0: TcpINBadParm

Explanation

Bad Parms in ParmLib.

04D1: TcpINCsvquery

Explanation

Bad RC from CSVQUERY macro.

04D2: TcpINPgser

Explanation

Bad RC from Pgser macro.

04D3: TcpINAxres

Explanation

Bad RC from Axres macro.

04D4: TcpINAsext

Explanation

Bad RC from Asext macro.

04D5: TcpINAsxTcbToken

Explanation

Bad RC from Tcbtoken.

04D6: TcpINLxfre

Explanation

Bad RC from Lxfre macro.

04D7: TcpINAttach

Explanation

Bad RC from Attach macro.

04D8: TcpINBadDelete

Explanation

Bad RC from Delete macro.

04D9: TcpINAxext

Explanation

Bad RC from Axext macro.

04DA: TcpINNoTseb

Explanation

No valid Tseb found.

04DB: TcpINBadDirectedLoad

Explanation

Bad RC from directed LOAD.

04DC: TcpInBadEZBITCOM

Explanation

EZBITCOM version does not match TCPIP version.

05C0: TcpS2Ecode

Explanation

Bad Entry code to module.

05C1: TcpSMLatchSetExists

Explanation

Storage Manager Latch Set already exists in this AS.

05C2: TcpSMLatchCreateOutOfStorage

Explanation

Storage Manager Latch Create out of storage.

05C3: TcpInIsglcrt

Explanation

Bad RC from Isglcrt service.

05C4: TcpInvCellStart

Explanation

Cell storage addr required.

05C5: TcpInAleserv

Explanation

Bad RC from Aleserv macro.

05C6: TcpInvReleaseReq

Explanation

Cannot do DSPSERV RELEASE for this cell pool.

05C7: TcpInCsrpbld

Explanation

Bad RC from Csrpbld service.

05C8: TcpInCsrpexp

Explanation

Bad RC from Csrpexp service.

05C9: TcpInvCellToken

Explanation

Cell pool token invalid.

05CA: TcpInvCellAddr

Explanation

Cell address is invalid.

05CB: TcpInCsrpget

Explanation

Bad RC from Csrpget service.

05CC: TcpInCsrpfre

Explanation

Bad RC from Csrpfre service.

05CD: TcpInCsrpqpl

Explanation

Bad RC from Csrpqpl service.

05CE: TcpInCsrpcon

Explanation

Bad RC from Csrpcon service.

05CF: TcpInCsrpact

Explanation

Bad RC from Csrpact service.

05D0: TcpCBInvalidStack

Explanation

A Storage Manager Control Block stack is invalid.

05D1: TcpCBStackOverflow

Explanation

A Storage Manager Control Block stack overflowed.

05D2: TcpOutOfMasterCells

Explanation

A Master Cell Pool is out of extent storage cells.

05D3: TcpOutOfMasterCBCells

Explanation

A Master Cell Pool is out of control block cells.

05D4: TcpOutOfStackCells

Explanation

A Cell Pool for stack storage is out of cells.

05D5: TcpInvalidCpoolId

Explanation

Expand stack invoked with an invalid cell pool ID.

05D7: TcpSmEstae

Explanation

Bad return code from Estae.

05D8: TcpInCsrpqex

Explanation

Bad RC from Csrpqex service.

05D9: TcpInCsrpdac

Explanation

Bad RC from Csrpdac service.

05DA: TcpInCsrpdis

Explanation

Bad RC from Csrpdis service.

05DB: TcpInLength

Explanation

Length of requested storage exceeds the maximum.

05DC: TcpInDataSpaceGroupID

Explanation

Invalid data space group ID is passed.

05DD: TcpInDataSpaceAlet

Explanation

Invalid data space alet is passed.

05DE: TcpInDataSpaceStoken

Explanation

Invalid data space Stoken is passed.

06C1: TcpTSEstae

Explanation

Bad RC from ESTAE macro.

06C2: TcpTCMLLockHeld

Explanation

CML lock held when it shouldnt be.

07C1: TcpLAObtHier

Explanation

Latch obtain hierarchy error.

07C3: TcpLARelHier

Explanation

Latch release hierarchy error.

07C5: TcpLAObtFail

Explanation

ISGLOBT Latch Obtain failure.

07C7: TcpLARelFail

Explanation

ISGLREL Latch release failure.

07C9: TcpLAFreLocked

Explanation

Cannot free latch - currently locked.

07CB: TcpLAInvTlcb

Explanation

Latch error - null Tlcb address or Tlcb Invalid.

07CD: TcpLAInvLmca

Explanation

Latch error - Lmca does not exist.

07CF: TcpLAInvLmqe

Explanation

Latch error - Lmqe does not exist.

07D1: TcpLAAllocLatch

Explanation

Cannot allocate latch from latch set.

07D3: TcpLAObtDelete

Explanation

Latch obtain failure - latch set marked deleted.

07D5: TcpLAInvConTok

Explanation

Invalid connection token for socket latch request.

07D7: TcpLAAllocLS

Explanation

Error allocated latch set

07D9: TcpLAInvTcb

Explanation

Tcb other than latch obtainer attempted latch release.

08C1: TcpSMGetCell

Explanation

Cell obtain failure - no more storage.

08C3: TcpSMGetCellD

Explanation

Cell obtain failure - cell pool marked for deletion.

08C5: TcpSMFreeCellZero

Explanation

Cell release failure - bad cell pointer.

08C7: TcpSMGetCellInUse

Explanation

Cell obtain failure - cell already in use.

08C9: TcpSMFreeCellInUse

Explanation

Cell release failure - cell not already in use.

08CB: TcpLALatchSetInUse

Explanation

Latch set delete failure - latch set already in use.

08CD: TcpSMFreeCellCirc

Explanation

Cell release failure - circular queue error.

08FF: TcpOPInvEye

Explanation

Invalid eyecatcher found in internal control block.

1001: TcpSKBadVerb

Explanation

Invalid verb passed to STREAMOP processor.

1101: TcpSKMsgNotAvailable

Explanation

Message triple is held or has been freed.

1102: TcpSKMsgHoldFailed

Explanation

Message triple is already held.

1103: TcpSKMsgReleaseFailed

Explanation

Message triple is already available.

2000: TcpitProcStackExceeded

Explanation

itProc size of dynamic storage area exceeded.

2001: TcpitLockObtNotInit

Explanation

Lock obtain - lockword not initialized.

2002: TcpitLockObtLevelHeld

Explanation

Lock obtain - cls/lvl already held for other lockword.

2003: TcpitLockObtStatusChange

Explanation

Lock obtain - attempt to change lock status shr- excl.

2004: TcpitLockObtHierarchy

Explanation

Lock obtain - level hierarchy violation.

2101: TcpitLockRelNotInit

Explanation

Lock release - lockword not initialized.

2102: TcpitLockRelNotHeld1

Explanation

Lock release - lock not held.

2103: TcpitLockRelLevelHeld

Explanation

Lock release - cls/lvl already held for other lockword.

2104: TcpitLockRelNotHeld2

Explanation

Lock release - lock not held.

2105: TcpitLockRelNotHeld3

Explanation

Lock release - lock not held.

2201: TcpitLockTstNotInit

Explanation

Lock test - lockword not initialized.

2301: TcpitLockRelAllAbend

Explanation

Lock release all-.

2401: TcpitLockSusError1

Explanation

Lock suspend - internal error.

2402: TcpitLockSusError2

Explanation

Lock suspend - internal error.

2403: TcpitLockSusError3

Explanation

Lock suspend - internal error.

2500: TcpitStorNoStorage

Explanation

No storage available – increase common storage. For more information on TCP/IP storage requirements and tuning, see informational APARs II11710, II11711, and II11712.

2501: TcpitStorNoCSMstorage

Explanation

No CSM storage available.

2502: TcpitStorBadHeader

Explanation

Bad storage header.

2503: TcpitStorBadTrailer

Explanation

Bad storage trailer.

2504: TcpitStorBadParm

Explanation

Bad storage input parameter.

2505: TcpitStorCSMtooLarge

Explanation

CSM storage request size too large.

2506: TcpitStorNotAllocated

Explanation

Release of storage not allocated.

2507: TcpitStorNoPrivStorage

Explanation

Failure allocating TCP/IP private storage.

2508: TcpitStorECSALimit

Explanation

Allocation would exceed ECSALIMIT in TCP/IP profile.

2509: TcpitStorPoolLimit

Explanation

Allocation would exceed POOLLIMIT in TCP/IP profile.

2600: TcpitDUbadParm

Explanation

SRB schedule - invalid ASCB.

2601: TcpitDUSusError1

Explanation

SRB suspend failure.

2701: TcpitTimerBadTQE1

Explanation

Timer cancel - invalid TQE.

2702: TcpitTimerCanError1

Explanation

Timer cancel - internal error.

2703: TcpitTimerCanError2

Explanation

Timer cancel - internal error.

2704: TcpitTimerBadTID1

Explanation

Timer cancel - invalid TID.

2705: TcpitTimerBadTQE2

Explanation

Timer pop/cancel - invalid TQE.

2706: TcpitTimerSetFailed

Explanation

Timer set - timer cannot be set.

2707: TcpitTimerBadState1

Explanation

Timer set - invalid state in TID.

2708: TcpitTimerBadTID2

Explanation

Timer cancel - invalid TID.

2709: TcpitTimerBadTQE3

Explanation

Timer cancel - invalid TQE.

270A: TcpitTimerBadState2

Explanation

Timer cancel - invalid state in TID.

2801: TcpitTrrStackFull

Explanation

Trr push - TRR stack full.

2900: TcpPatTreeCorrupted

Explanation

Patricia tree structure was corrupted.

2901: TcpPatTreeKeyTooLarge

Explanation

Patricia tree key length is too large.

2902: TcpPatTreeBadParm

Explanation

Bad PatTree input parameter.

2A00: TcpHashTabUnbalanced

Explanation

A Hash Table Find was done but was not followed by a FindComplete.

3001: TcpSTKattLoop

Explanation

Loop detected in ATT entries.

3002: TcpSTKblkngArrInvalid

Explanation

Invalid Manipulation of the Blocking Array.

3003: TcpSTKPtreeRecovery

Explanation

Abend while in the Routing Patricia Tree.

3004: TcpSTKLoopIutlChain

Explanation

Loop in IUT plist chain was detected.

3005: TcpSTKMProtoInvalid

Explanation

Corrupted MPROTO detected.

3006: TcpSTKLoopIutlDChain

Explanation

Loop in QDIO IUT plist chain was detected.

3007: TcpSTKLoopXbflChain

Explanation

Loop in buffer list chain was detected.

3009: TcpIEBegProfTimer

Explanation

Profile processing did not complete. Recycle the TCP/IP stack as soon as possible because the configuration of the stack might not be stable.

300A: TcpNmiBadRetInfo

Explanation

The NMI return value, the code variables, and reason variables were not addressable.

300B: TCPDvipaError

Explanation

IP address control blocks were missing for new DVIPA interfaces.

3100: TcpPascalUnexpectCond

Explanation

RC of SoftwareError indicates an APAR condition.

3101: TcpPascalUnknownFnCode

Explanation

PC Router called with invalid function code.

3133: TcpTelnetAbendTrap

Explanation

Abend Trap for Telnet error was set.

3134: TcpTelnetStall

Explanation

Telnet stall detected.

3202: TcpTestNoNSwap

Explanation

The address space is nonswappable.

User response

Find the entry for the abending program in the program properties table in your SCHEDxx SYS1.PARMLIB member. Ensure that the SWAP attribute is set for the entry.

3203: TcpTestSwap

Explanation

The address space is swappable.

3204: TcpTestNoCancel

Explanation

The address space is noncancelable, but the program is not marked noncancelable.

User response

Find the entry for the abending program in the program properties table in your SCHEDxx SYS1.PARMLIB member. Ensure that the NOCANCEL attribute is set for the entry.

3205: TcpTestCancel

Explanation

The address space is cancelable.

3210: TcpTestPSWsuper

Explanation

The current PSW is in supervisor state.

3211: TcpTestPSWPgm

Explanation

The current PSW is in program state.

3213: TcpTestPSWUserKey

Explanation

The current PSW indicates a user key (8-F).

3214: TcpTestPSWSysKey

Explanation

The current PSW indicates a system key (0-7).

3215: TcpTestPSWBadKey

Explanation

The current PSW indicates an incorrect key.

User response

The program is not executing in the correct key. Find the entry for the abending program in the program properties table in your SCHEDxx SYS1.PARMLIB member. Ensure that the correct KEY attribute is set for the entry.

3216: TcpTestAPF1

Explanation

Program is executing with APF 1.

3217: TcpTestAPF0

Explanation

Program is executing with APF 0.

User response

The program is not executing with an authorization code of 1 (AC=1). Verify that the program has been link edited correctly and is executing from an APF-authorized library.

3221: TcpTestTask

Explanation

Program is executing in task mode.

3222: TcpTestSRB

Explanation

Program is executing in SRB mode.

3223: TcpTestJobStep

Explanation

Program is not executing as a job step task.

3224: TcpTestTobJob

Explanation

Program is not executing as the first job step task.

3225: TcpTestAmode24

Explanation

Program is not executing in AMODE 24.

3226: TcpTestAmode31

Explanation

Program is not executing in AMODE 31.

3227: TcpTestAmode64

Explanation

Program is not executing in AMODE 64.

3230: TcpTestSys

Explanation

The address space is not a system address space.

3231: TcpTestSTC

Explanation

The address space is not a started task.

User response

The program was not started as a system task. Find the entry for the abending program in the program properties table in your SCHEDxx SYS1.PARMLIB member. Ensure that the SYST attribute is set for the entry. Verify that a START command was used to start this program.

3232: TcpTestInit

Explanation

The address space is not an initiated job.

3233: TcpTestTSO

Explanation

The address space is not a TSO address space.

3235: TcpTestOMVS

Explanation

The address space is not an OMVS address space.

3236: TcpTestAPPC

Explanation

The address space is not an APPC address space.

3237: TcpTestUID0

Explanation

The address space does not have a UID of zero.

User response

Change the RACF/SAF definition of the OMVS segment to UID(0).

C001: TcpJCodeNotValid

Explanation

The callable service is incorrect or is not supported.

C009: ResBadReturnInfo

Explanation

Resolver service was unable to set the return value, return code, or reason code.

Chapter 17. FTPD reply codes

Each time an FTP client sends an FTP command to the FTP server, that FTP server responds with one or more replies. Replies are in the format:

xyz text
or
xyz- text

where:

xyz
An architected reply code of three digits in the range 100-599. Each digit of the code is significant; its meaning is described in RFC 959, *File Transfer Protocol*. In practice, the leading digit is most significant. A dash following the reply code (xyz-) indicates that the reply cannot fit in a single line and more lines of the same reply code are expected. The last line of the reply code does not have the dash.

text
Humanly-readable text that explains the meaning of the reply code.

Rule: The humanly-readable text portion of an FTP reply is not a programming interface. For more information, see RFC 959, section *4.2. FTP REPLIES*. Other servers might return different humanly-readable text in similar scenarios, and the z/OS FTP server reply texts are subject to change.

Reply codes are listed first in numerical order by the *xyz* value, then alphabetically by the first token in *text*.

The following list shows an overview of xyz values:

100 - 159
Replies in this range are informational messages and are usually followed by another reply that is in another range. An example of a reply of this type is `125 Sending data set /etc/hosts`, which is sent after the client sends a RETR command to the server to fetch /etc/hosts.

200 - 259
Replies in this range indicate that the command that the client sent to the server completed successfully.

300 - 359
Replies in this range indicate that the command that the client sent to the server has been accepted by the server, but more information is needed to complete this request. An example of a reply in this range is `350 RNFR accepted. Please supply new name for RNTO.`, which is sent after the client sends a RNFR (rename from) command to the server.

400 - 459
Replies in this range indicate that the client's request was denied; however, the error is temporary and the client can request the action again.

500 - 559
Replies in this range indicate that the client's request failed because of a permanent error. Repeating the request in the identical sequence is not likely to succeed.

The significance of the second digit is architected by RFC 959 as follows:

x0z
If the second digit is **0**, a syntax error was detected in the command that the client sent to the server.

x1z
If the second digit is **1**, the reply contains information that was requested by the client.

x2z
If the second digit is **2**, the reply contains information relating to the control or data connection.

© Copyright IBM Corp. 2000, 2021

x3z
If the second digit is **3**, the reply is part of the login sequence or another authentication sequence.

x4z
A second digit of **4** is not in current use.

x5z
If the second digit is **5**, the reply contains server file system information relevant to the last command that the client sent to the server.

This topic describes the reply codes that the z/OS FTP server generates. For codes that can be issued from other FTP servers, see the documentation that other vendor platforms provide. The codes must conform with the structure that is defined in RFC 959.

See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

125 reply codes

125: Appending to data set *name*

Explanation

The current data set is being appended to the indicated data set.

System action

FTP continues.

User response

None.

System programmer response

None.

125 : Appending to named pipe *pathname*

Explanation

The FTP server received an APPE (append) or STOR (store) file transfer command while UNIXFILETYPE=FIFO was configured. The FTP server is appending the incoming data to the specified named pipe.

Storing into a named pipe never overwrites the contents of the named pipe; it always appends the data to the existing contents. When the named pipe specified by the *pathname* value is empty, the effect of appending is the same as storing.

See the UNIXFILETYPE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference for more information about the UNIXFILETYPE configuration option.

In the message text:

pathname
The name of the named pipe.

Example

```
Command:
site unixfiletype=fifo
>>> SITE unixfiletype=fifo
```

```
200 SITE command was accepted
Command:
put /etc/hosts /tmp/etc.hosts.fifo
>>> PORT 9,2,1,3,4,33
200 Port request OK.
>>> STOR /tmp/etc.hosts.fifo
125 Appending to named pipe /tmp/etc.hosts.fifo
250 Transfer completed successfully.
41 bytes transferred in 0.005 seconds.  Transfer rate 8.20 Kbytes/sec.
Command:
```

System action

FTP appends data to the named pipe.

User response

If you intended to transfer data into a named pipe, no further action is needed.

If you intended to transfer data into a regular z/OS UNIX file, use the SIte subcommand to change the UNIXFILETYPE configured value at the FTP server, and transfer the file again. See the information about the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands .

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

125-: Binary tagged file translated with current data connection translation table

Explanation

The file that is to be transferred was tagged binary but the data type is ASCII. This is a warning to the user that the file will be translated.

System action

The file transfer continues.

User response

If it is acceptable that the file was translated to ASCII during the transfer, then no action is necessary. However, if no translation should have been done, change the transfer type to binary and transfer the file again. See the z/OS UNIX System Services Command Reference for information about the CHTAG command. See the z/OS Communications Server: IP User's Guide and Commands for information about the FTP TYPE subcommand.

System programmer response

None.

125: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

125: Could not allocate receive buffer

Explanation

A command was issued to retrieve output from JES. A buffer required for this command to process is not available.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be sent.

User response

None.

System programmer response

None.

125: Data connection already open; transfer starting.

Explanation

The FTP server is about to transfer data. The server determined that a data connection already existed and it was not necessary to open a new data connection. The FTP server will use the existing data connection for FTP transfer.

System action

FTP continues.

User response

None.

System programmer response

None.

125-: Data set access will be retried in 1 minute intervals - *number* attempts remaining

Explanation

The client sent the RETR, STOR, or APPE command to the FTP server; however, the MVS data set that is specified by the command is being held by one or more jobs.

This reply is part of a sequence of 125- replies. This reply is issued every *DSWAITTIMEREPLY* seconds when the server is waiting to obtain the data set. This reply indicates how many more times the FTP server can attempt to access the MVS data set.

In the reply text:

number
The remaining number of times that the FTP server can attempt to access the MVS data set.

Example

```
ftp> get 'USER1.FTPDATA' testing
200 Port request OK.
125-FTP Server unable to obtain SHARED use of USER1.FTPDATA which is held by: 005C MYJOB EXCLUSIVE SYSDSN
125-Data set access will be retried in 1 minute intervals - 1 attempts remaining
125 Sending data set USER1.FTPDATA
250 Transfer completed successfully.
```

System action

The FTP server continues to try to access the MVS data set.

User response

If you need immediate access to the MVS data set, contact the system programmer for the FTP server and provide the sequence of 125- replies.

System programmer response

Perform the following actions:

1. Use the information in the 125- replies or in message EZZ9819I in the SYSLOGD file to determine which job or jobs are holding the MVS data set and resolve the contention.
2. Purge or cancel the job that is causing the MVS data set contention, if appropriate.
3. Modify the DSWAITTIME configuration statement in the server FTP.DATA file based on your end-user requirements and recycle the FTP server to cause the change to take effect for new FTP sessions. See the information about the DSWAITTIME statement in z/OS Communications Server: IP Configuration Reference.

   Tip: You can change the DSWAITTIME configured value for the current session only by sending a SITE command to the server with the DSWAITTIME parameter. See the information about the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands .

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

125: Data set *dsname* is migrated and NoAutoRecall is specified.

Explanation

A submit job request was received for a job located in a data set at the server. The data set was migrated and needed to be recalled. The FTP server is currently in NoAutoRecall mode.

System action

The command is rejected.

User response

Issue the SITE AUTORECALL command to allow the data set to be recalled, and then reissue the FTP command.

System programmer response

None.

125: Data set *dsname* is not available

Explanation

The FTP server received an FTP command that required access to an MVS data set name that is being held by one or more jobs. This is the closing reply for a sequence of 125- replies. The sequence identifies the jobs that are holding the MVS data set, and the number of MVS data set access attempts that remain. The FTP server attempted to access an MVS data set in approximately 1-minute intervals for the amount of time specified in the DSWAITTIME statement in the FTP server FTP.DATA file. The contention for the MVS data set could not be resolved and the command is rejected.

In the reply text:

dsname
The name of the MVS data set that is not available because it is held by other jobs.

Example

```
get 'user1.ftpdata' testfile
 EZA1701I >>> PORT 127,0,0,1,4,5
 200 Port request OK.
 EZA1701I >>> RETR 'user1.ftpdata'
200 Port request OK.
125-FTP Server unable to obtain SHARED use of USER1.FTPDATA which is held by: 005C MYJOB EXCLUSIVE SYSDSN
125-Data set access will be retried in 1 minute intervals - 1 attempts remaining
125 Data set USER1.FTPDATA is not available
450 Data set USER1.FTPDATA is allocated to another job and is unavailable for RETR command.
EZA1460I Command:
```

System action

The file transfer fails and processing continues.

User response

Do one of the following actions:

- Use the STAT command to determine the DSWAITTIME value for this session from the FTP server perspective. Use the SITE command to change the DSWAITTIME value and try the file transfer again.

For example, from the z/OS FTP client, issue the following subcommand to set the total time to wait for the MVS data set to become available to 10 minutes:

```
SITE DSWAITTIME=10
```

See the information about using the STAT subcommand and SIte subcommand in z/OS Communications Server: IP User's Guide and Commands and the DSWAITTIME statement in z/OS Communications Server: IP Configuration Reference.

- Transfer the file when the MVS data set is available.
- If you need immediate access to the MVS data set, contact the system programmer and provide the sequence of 125- replies

System programmer response

Perform the following actions:

1. Use the information in the 125- replies to determine which job or jobs are holding the MVS data set and resolve the contention.
2. Purge or cancel the job causing the MVS data set contention, if appropriate.
3. Modify the DSWAITTIME in your FTP.DATA file based on your end-user requirements, and recycle the FTP server for the change to take effect for new FTP sessions.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

125: *dsname* is a physical sequential data set and a member was specified on the RETR command.

Explanation

The client entered the RETR command to request that a JES job be submitted and the output of the job retrieved. The path name on the RETR command indicated that the job to be submitted was a member of the MVS partitioned data set *dsname*, but the FTP server determined that *dsname* was a physical sequential data set, and not a partitioned data set.

System action

The command is rejected. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125: DCB *lrecl blksize*

Explanation

This message contains the DCB parameters that will be required for the client to replicate the temporary file containing unloaded load modules, which the server is preparing to send to the client.

lrecl
The logical record length required for the temporary data set

blksize
The block size required for the temporary data set

System action

FTP continues.

User response

None.

System programmer response

None.

125: Error allocating tape data set *dsname*

Explanation

The server attempted to allocate to a data set on a tape volume. The dynamic allocation was unsuccessful.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

Examine the trace and look for trace messages with the tag *alloc_tape*. These trace messages provide the reason codes for the dynamic allocation error.

125: Error mounting volume

Explanation

A request was received that requires a data set at the server. The data set will be allocated on a volume that is not mounted. The FTP server attempted to mount the volume but was unable to successfully do so.

System action

The command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Determine why the volume cannot be mounted and correct the problem.

125: Error mounting volume containing data set *dsname*

Explanation

A request was received that requires a data set at the server. The data set is on a volume that is not mounted. The FTP server attempted to mount the volume but was unable to successfully do so.

System action

The command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Determine why the volume cannot be mounted and correct the problem.

125: error occurred while seeking restart marker

Explanation

The server attempted to restart a store operation, as requested by the client. However, an error occurred when the server was positioning its file marker. The file transfer is ended.

System action

Processing continues.

User response

Contact the system programmer with the error.

System programmer response

Contact the IBM Software Support Center with the error.

125: Error recalling data set *dsname*.

Explanation

The command being processed requires a data set at the server. The data set was migrated and needed to be recalled. The FTP server attempted to recall the data set, but was unable to successfully recall it.

System action

The command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Determine why the data set cannot be recalled and correct the problem.

125: Error recalling data set *data_set* (rc=*rc*)

Explanation

The command being processed requires a data set at the server. The data set was migrated and needed to be recalled. The FTP server attempted to recall the data set, but was unable to successfully recall the data set.

rc is the return code from the ARCHRCAL macro. See the z/OS DFSMShsm Managing Your Own Data for information about ARCHRCAL return codes.

System action

The command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Determine why the data set cannot be recalled and correct the problem.

125: File *dsname* not found.

Explanation

The job was not submitted because the file was not found.

System action

The job is not submitted. FTP continues.

User response

Reissue the request with a name of a file that can be found by the server. To ensure that the server can find the file, issue a DIR subcommand for the file after issuing SITE FILETYPE=SEQ.

System programmer response

None.

125: *file_name* request nonexistent member to be sent.

Explanation

A command was issued specifying resource *file_name* The resource appears to be a member of a partitioned data set, but the member does not exist in the specified PDS.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be presented by the server.

User response

Reissue the command with a correct *file_name* or PDS member name.

System programmer response

None.

125-: Format of file number incorrect, *filenum* ignored.

Explanation

The RETR command is being executed with the specified job ID and all files. The job ID must be in the form of JOBxxxxx, TSUxxxxx, APCxxxxx, TSUxxxxx or JOBxxxxx.y, TSUxxxxx.y, APCxxxxx.y, TSUxxxxx.y to retrieve a file. Note that the file number postfix can be either the string ".X" or .1 through the number of files assocated with the job. The file number postfix .0 is an incorrect value.

System action

The file number is ignored and the RETR command is executed for all files.

User response

None.

System programmer response

None.

125-: FTP Server unable to obtain *type* use of *dsname* which is held by: *asid jobname accessmode* on *qname*

Explanation

The FTP server received an FTP command that required access to an MVS data set name that is being held by one or more jobs. This reply is sent as part of a sequence of replies that identify some of the jobs that are holding the MVS data set. This reply can be suppressed by enabling the REPLYSECURITYLEVEL configuration option.

If FTP is unable to determine which job is holding the resource, the *asid*, *jobname*, *accessmode*, and *qname* values will be UNKNOWN. Some of the conditions that can cause FTP to be unable to determine which job is holding the resource are:

- The resource is being held by a job that is running on another processor.
- The device on which the data set resides prohibits access to the MVS data set.

In the reply text:

type
The type of access that FTP was attempting to obtain. Possible values are:

EXCLUSIVE
FTP requires the exclusive use of the MVS data set.

SHARED
FTP requires the shared use of the MVS data set.

dsname
The name of the MVS data set being held by another job.

asid
The address space identifier of the job holding the MVS data set. If FTP cannot identify the job that is holding the data set, the *asid* value is UNKNOWN.

jobname
The job name associated with an address space identifier (ASID) that is holding the MVS data set. If FTP cannot identify the job that is holding the data set, the *jobname* value is UNKNOWN.

accessmode
The way the MVS data set is being held. Possible values are:

EXCLUSIVE
A job is accessing the data set exclusively.

SHARED
A job is accessing the data in shared mode.

UNKNOWN
FTP is unable to identify the job that is holding the data set.

qname
The name of the queue used by the enqueue operation. Possible values are:

SPFEDIT
The queue used by ISPF EDIT, FTP, and other processes when access to a member of an MVS partitioned data set is required.

SYSDSN
The queue used by z/OS when access to an MVS data set is required.

UNKNOWN
FTP cannot identify the job that is holding the data set.

See ISPF or ISPF/PDF in z/OS MVS Planning: Global Resource Serialization for information about how MVS serializes the use of resources and the use of SPFEDIT.

Example

```
ftp> get 'USER1.FTPDATA' testing
200 Port request OK.
125-FTP Server unable to obtain SHARED use of USER1.FTPDATA which is held by: 005C MYJOB EXCLUSIVE SYSDSN
125-Data set access will be retried in 1 minute intervals - 1 attempts remaining
125 Sending data set USER1.FTPDATA
250 Transfer completed successfully.
```

System action

The FTP server continues to try to access the local MVS data set.

User response

If you need immediate access to the MVS data set, contact the system programmer for the FTP server and provide the sequence of 125- replies.

System programmer response

Perform the following actions:

1. Use the information in the 125- replies to determine which job or jobs are holding the MVS data set and resolve the contention.

2. Purge or cancel the job causing the MVS data set contention, if appropriate.
3. Modify the DSWAITTIME configuration statement in your FTP.DATA file based on your end-user requirements, and recycle the FTP server for the change to take effect for new FTP sessions.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: Health Checker

125: Invalid data set name *"dsname"*. Use MVS Dsname conventions.

Explanation

The data set name violates one of the MVS file naming conventions and cannot be used to reference a data set at the server.

System action

The job is not submitted. FTP continues.

User response

Rename the data set in compliance with MVS data set naming conventions. For more information about MVS data set naming conventions, see the z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

125: JES internal reader *operation* failed

Explanation

In preparation of submitting a job to MVS the Internal Reader needed to be allocated or opened. This operation of the Internal Reader failed.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125: List started OK for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner*

Explanation

The LIST command is being executed with the specified SITE parameters. The server is getting ready to transfer the LIST command output back to the client.

System action

The LIST command is executed.

User response

None.

System programmer response

None.

125: List started OK

Explanation

The LIST or NLST command is being executed. The server is getting ready to transfer the LIST or NLST command output back to the client.

System action

The LIST or NLST command is executed.

User response

None.

System programmer response

None.

125: List terminated.

Explanation

The FTP server was preparing to transfer the output from the LIST or NLST command, but encountered an error and ended the data transfer. This reply is followed by a 550 reply with additional information about the error.

System action

The data transfer ends.

User response

None.

System programmer response

None.

125: Mismatched quotes on pathname *pathname*

Explanation

The path name provided for a data set that contains a job to submit was enclosed in an unbalanced set of single quotes.

System action

The job is not submitted. FTP continues.

User response

Enclose the data set name in balanced quotes -- a quote at the beginning and the end of the name.

System programmer response

None.

125: Name length error for pathname *pathname*

Explanation

The path name provided for a data set that contains a job to submit is too long. The name, when combined with the current working directory, must adhere to the following maximum lengths:

- 44 for a physical sequential data set
- 55 for a member of a PDS (includes the parentheses for the member name
- 1023 for a file in the hierarchical file system.

  Note: The maximum length for a file name is 255 -- the total path name maximum length is 1023.

System action

The job is not submitted. FTP continues.

User response

Reissue the request with a name that meets the limits for the type of data set or file.

System programmer response

None.

125: Nlst started OK

Explanation

A command was issued to obtain an NLST. The NLST command started ok.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be sent.

User response

None.

System programmer response

None.

125: Nlst started OK for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner*

Explanation

The NLST command is being executed with the specified SITE parameters. The server is getting ready to transfer the NLST command output back to the client.

System action

The NLST command is executed.

User response

None.

System programmer response

None.

125: Non-DASD data set *dsname* cannot be processed.

Explanation

A command was issued against a data set that does not reside on a Direct Access Storage Device (DASD).

System action

FTP server continues normal execution. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125: Open of *dsname* failed.

Explanation

The data set or file containing a job cannot be opened.

System action

The job is not submitted. FTP continues.

User response

None.

System programmer response

If necessary, re-create the problem with FTP server trace active. The open file error will create a trace record with an *errno* code. Determine the cause of the error and correct the problem. *errno* is the z/OS UNIX System Services Return Code. These return codes are listed and described in the z/OS UNIX System Services Messages and Codes.

125: Retrieve of a whole Partitioned data set is not supported. Use MGET for this purpose.

Explanation

The client entered the RETR command to request that a JES job be submitted and the output of the job retrieved. The path name on the RETR command indicated that the job to be submitted was the MVS data set *dsname*, but the FTP server determined that *dsname* was a partitioned data set, which requires a member name to be specified with *dsname*.

System action

The command is rejected. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125-: Seeking restart marker

Explanation

The server is restarting a store operation, as requested by the client. The server is positioning its file marker at the location specified on the last REST command.

System action

Processing continues.

User response

None.

System programmer response

None.

125: 125 Sending all spool files for requested Jobid

Explanation

The FTP server is sending all the files in the spool for a specified job ID. For more information about spool files, see the z/OS Communications Server: IP User's Guide and Commands.

System action

The files are sent. FTP continues.

User response

None.

System programmer response

None.

125: Sending data set *data set* FIXrecfm *record length*

Explanation

The FTP server is sending the indicated data set with a fixed record length. The record length is indicated in the reply.

System action

The data set is transferred. FTP continues.

User response

None.

System programmer response

None.

125: Sending data set *name*

Explanation

The FTP server is sending the indicated data set.

System action

FTP continues.

User response

None.

System programmer response

None.

125: Sending file via NJE to requested destination.

Explanation

The data that is transferred from the client is being sent via Network Job Entry (NJE) to the destination specified by the SITE DEST= parameter.

System action

FTP continues.

User response

None.

System programmer response

None.

125: Sending Job to JES internal reader *format record length*

Explanation

The FTP server is sending the indicated job to the job entry system (JES) internal reader with the indicated record format and record length. For more information on JES, see the z/OS Communications Server: IP User's Guide and Commands.

System action

The job is sent to JES. FTP continues.

User response

None.

System programmer response

None.

125: Storing data in the Null directory (*dev.null).

Explanation

The FTP server is transferring data from the client but is not storing the data in the file system. This action was requested with a change directory command to the null directory.

System action

FTP continues.

User response

None.

System programmer response

None.

125: Storing data set *name*

Explanation

The FTP server is storing the indicated data set. If the data set already exists, it is replaced by the transferred data.

System action

FTP continues.

User response

None.

System programmer response

None.

125: Storing data set *name* (unique name)

Explanation

The FTP server is storing the indicated data set with a unique name. This prevents overwriting or erasure of existing files on the remote host.

System action

FTP continues.

User response

None.

System programmer response

None.

125: Submit fails: *dsname* User not authorized.

Explanation

The job was not submitted. The requested data set is protected by a security system such as RACF, and the user is not authorized to read the data set.

System action

The job is not submitted. FTP continues.

User response

Contact the owner of the data set for authorization to read the data set.

System programmer response

None.

125-: Submitting job *job_id format record_length*

Explanation

The indicated job is being submitted to the Job Entry System (JES).

System action

The job is submitted. FTP continues.

User response

None.

System programmer response

None.

125-: Tagged *type* file translated with table built using file system cp=*codepage_1*, network transfer cp=*codepage_2*

Explanation

The FTP server detected that the local file is tagged with a coded character set ID (ccsid). A translation table is built for this data transfer using the codepage that corresponds to the ccsid.

type is either ASCII or EBCDIC.

codepage_1 is the codepage of the file.

codepage_2 is the codepage that was specified for the network transfer codepage on SITE SBDATACONN or on the SBDATACONN statement in the FTP.DATA file.

System action

FTP continues.

User response

None.

System programmer response

None.

125-: Tagged *type* file translated with current data connection translation table

Explanation

The FTP server detected that the local file is tagged with a coded character set ID (ccsid). The data connection translate table is not defined with the SBDATACONN=(file_system_cp,network_transfer_cp) method. Without a network transfer codepage, the server cannot build a translate table using the ccsid of the file. The FTP server uses the translate table defined for the data connection.

type is either ASCII or EBCDIC.

System action

FTP continues.

User response

None.

System programmer response

None.

125: Transfer aborted: file error.

Explanation

A file error occurred while processing the command.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125: Transfer aborted: send error.

Explanation

While attempting to submit a job from the command, the data connection was lost. The job might or might not have been successfully submitted to the system for processing.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125: Transfer request aborted

Explanation

The FTP server closed the data connection because of an internal error. This reply ends an outstanding preliminary reply.

System action

FTP continues.

User response

None.

System programmer response

None.

125-: Transferring load module

Explanation

The RETR command is being executed, and the server is preparing to send a temporary data set containing unloaded load modules to the client.

System action

FTP continues. A second 125 message will be sent containing DCB parameters for the temporary file.

User response

None.

System programmer response

None.

125: Transferring load module

Explanation

The STOR command is being executed, and the server is preparing to receive a temporary data set containing unloaded load modules from the client.

System action

FTP continues.

User response

None.

System programmer response

None.

125: Unable to get Jobid

Explanation

GET command with automatic retrieve was issued. The job ID could not be obtained after being submitted.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be sent.

User response

None.

System programmer response

None.

125: Unable to send *name*

Explanation

The file used in a JesPutGet operation either cannot be found, is being used by another process, or cannot be opened.

System action

FTP continues.

User response

None.

System programmer response

None.

125: User Exit refuses this Job to be submitted by *dsname*

Explanation

During the submit of a job to JES, a JES user or installation exit encountered an error. The request to submit the job might have failed.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125: Volume containing *dsname* is not mounted and NoAutoMount specified.

Explanation

A submit job request was received for a job located in a data set at the server. The data set is on a volume that is not mounted. The FTP server is currently in NoAutoMount mode.

System action

The command is rejected.

User response

Issue the "SITE AUTOMOUNT" command to allow the volume to be mounted, and then reissue the FTP command.

System programmer response

None.

125: Volume is not ready and automatic tape mounts are not allowed.

Explanation

A request to retrieve a data set from or store a data set on a tape volume was received. The tape volume is not mounted and the end user requested NoAutoTapeMount.

System action

The request is not performed.

User response

Request that the tape be mounted by the operator and then reissue the request. Also, the SITE AUTOTAPEMOUNT subcommand can be issued to allow automatic tape mounts to occur.

System programmer response

None.

125: VSAM data set *dsname* cannot be processed.

Explanation

A command was issued that requests action be performed against a VSAM data set. VSAM data sets are not supported.

System action

FTP server continues normal execution. The FTP client waits for the next reply to be presented by the server.

User response

None.

System programmer response

None.

125: wait ended

Explanation

The FTP server previously issued a 125 message indicating a wait state, such as 125-waiting for recall of data set. The anticipated event has ended.

System action

The FTP server continues processing the current command.

User response

None.

System programmer response

None.

125-: Waiting for allocation of tape data set *dsname*

Explanation

A retrieve or store command was issued for a data set that is on a tape volume. The FTP server might have to have the volume mounted. The server will wait for the volume to be successfully mounted and then begin processing the data set.

System action

The FTP server prompts the operator to mount the volume. FTP processing continues once the volume is mounted.

FTP continues.

User response

None.

System programmer response

None.

125-: Waiting for batch pipe subsystem *name* reader to open

Explanation

You attempted to transfer a file to the FTP server while SUBSYS was configured. The SUBSYS parameter specified the name of a BatchPipes® subsystem. When SUBSYS specifies the name of a BatchPipes subsystem, the server data set name is a pipe. The BatchPipes reader has not opened the data set yet.

In the reply text:

name
The name of the BatchPipes subsystem that is specified on the SUBSYS parameter of the SITE command.

Example

```
ftp> site subsys=bp01
ftp> type I
ftp> put 'user.data'
125-Waiting for batch pipe subsystem bp01 reader  to open
125 Storing data set USER.DATA
250 Transfer completed successfully.
```

System action

FTP waits until the BatchPipes reader has opened the data set.

Operator response

Start the BatchPipes reader, if necessary. If this does not resolve the problem, contact the system programmer.

User response

If processing does not continue, contact the operator.

System programmer response

If starting the BatchPipes subsystem and the BatchPipes reader does not resolve the problem, enable the FTP server traces and contact the IBM Support Center.

See the information about documenting server problems in z/OS Communications Server: IP Diagnosis Guide.

Problem determination

See the system programmer response. See z/OS MVS JCL Reference for information about the SUBSYS parameter.

Source

Not applicable.

Module

Not applicable.

Routing code

Not applicable.

Descriptor code

Not applicable.

125-: Waiting for read process to open *pathname*

Explanation

The FTP server received a STOR (store) or APPE (append) command that specified a named pipe as the target file. The FTP server must wait for another process to open the named pipe in read mode before the server can process the STOR or APPE command.

This reply is one of a sequence of replies that are sent to the FTP client when the FTP server must wait for another process to open a named pipe in read mode.

See the information about using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User's Guide and Commands.

In the message text:

pathname
The name of the named pipe.

Example

```
Command:
put /etc/hosts /tmp/etc.hosts.fifo
>>> PORT 9,2,1,3,4,35
200 Port request OK.
>>> STOR /tmp/etc.hosts.fifo
125-Waiting for read process to open /tmp/etc.hosts.fifo
125 Transfer request
aborted

450 timer expired waiting for read process to open /tmp/
etc.hosts.fifo
Command:


Command:
put /etc/hosts /tmp/etc.hosts.fifo
>>> PORT 9,2,1,3,4,36
200 Port request OK.
>>> STOR /tmp/etc.hosts.fifo
125-Waiting for read process to open /tmp/etc.hosts.fifo
125 Appending to named pipe /tmp/etc.hosts.fifo
250 Transfer completed successfully.
41 bytes transferred in 0.005 seconds.  Transfer rate 8.20 Kbytes/sec.
Command:
```

System action

The FTP server waits up to the number of seconds specified by the FIFOOPENTIME configuration option for the read process to open the path specified by the *pathname* value.

User response

Notify the system administrator of the server host to start the process that writes to the named pipe.

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

125-: Waiting for recall of data set *data set*

Explanation

A command was issued for a data set that is migrated. The FTP server must recall the data set in order complete the command. The server waits for the data set to be successfully recalled and then begins processing the command.

System action

The FTP server recalls the data set. FTP continues.

User response

None.

System programmer response

None.

125-: Waiting for volume mount for *dsname*

Explanation

A command was issued for a data set that is catalogued on a volume that is not mounted. The FTP server must mount the volume in order to complete the command. The server waits for the volume to be successfully mounted and then begins processing the command.

System action

The FTP server prompts the operator to mount the volume. FTP processing continues once the volume is mounted.

User response

None.

System programmer response

None.

125-: Waiting for volume mount for volume *volume*

Explanation

The FTP server is waiting for the volume to be mounted. The FTP server is about to open the data connection.

System action

FTP continues. The FTP server mounts the volume automatically.

User response

None.

System programmer response

None.

125-: Waiting for write process to open *pathname*

Explanation

The FTP server received a RETR (retrieve) command that specified a named pipe as the file to retrieve from the server file system. The FTP server must wait for another process to open the named pipe in write mode before the server can process the RETR command.

This reply is one of a sequence of replies that are sent to the FTP client when the FTP server must wait for another process to open a named pipe in write mode.

See the information about using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User's Guide and Commands.

In the message text:

pathname
The name of the named pipe.

Example

```
Command:
get /tmp/etc.hosts.fifo /etc/hosts
>>> PORT 9,2,1,3,4,35
200 Port request OK.
>>> RETR /tmp/etc.hosts.fifo
125-Waiting for write process to open /tmp/etc.hosts.fifo
125 Transfer request aborted
450 timer expired waiting for write process to open /tmp/etc.hosts.fifo
Command:
```

System action

The FTP server waits up to the number of seconds specified by the FIFOOPENTIME configuration option for the write process to open the path specified by the *pathname* value.

User response

Notify the system administrator of the server host to start the process that writes to the named pipe.

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

125-: Warning TAPEREADSTREAM configured - <NL> in data cannot be translated

Explanation

The server received a RETR command to retrieve a tape data set when TAPEREADSTREAM is configured. The tape data set appears to meet the requirements for the TAPEREADSTREAM configuration. However, if the tape data set contains <NL> characters, FTP cannot translate the <NL> characters correctly so the format might be incorrect.

System action

The file transfer continues.

User response

If the transferred data set format is not correct, choose one of these solutions:

- If your client is a z/OS Communications Server FTP client, issue a SITE NOTAPEREADSTREAM subcommand to change the value for the current session. Then retrieve the tape data set again.
- If your client is not a z/OS Communications Server FTP client, issue a QUOTE SITE NOTAPEREADSTREAM subcommand to change the value for the current session. Then retrieve the tape data set again.

For more information about the SIte subcommand, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

To change the TAPEREADSTREAM value permanently, change the TAPEREADSTREAM statement in FTP.DATA. For more information about the TAPEREADSTREAM statement, see z/OS Communications Server: IP Configuration Reference.

125: When *job_id* is done, will retrieve its output

Explanation

When the indicated job is completed, the FTP server will retrieve the output from the Job Entry System (JES). If the specified job id is "*UNKNOWN", the retrieval of the job identifer from JES failed.

System action

FTP continues.

User response

None.

System programmer response

None.

150 reply codes

150: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

150: Waiting for allocation of tape data set *dsname*

Explanation

A retrieve or store command was issued for a data set that is on a tape volume. The FTP server might have to have the volume mounted. The server will wait for the volume to be successfully mounted and then begin processing the data set.

System action

The FTP server prompts the operator to mount the volume. FTP processing continues once the volume is mounted.

FTP continues.

User response

None.

System programmer response

None.

150: Waiting for recall of data set *dsname*

Explanation

The FTP server is waiting for the recall of the indicated data set. The FTP server will open a data connection for the data transfer.

System action

The FTP server recalls the data set. FTP continues.

User response

None.

System programmer response

None.

150: Waiting for volume mount for *dsname*

Explanation

The FTP server is waiting for the volume containing the indicated data set to be mounted. The FTP server is about to open the data connection.

System action

FTP continues. The FTP server mounts the volume automatically.

User response

None.

System programmer response

None.

200 reply codes

200-: Active server dumpIDs -*value_1 value_2 ... value_n*

Explanation

The SITE command was specified with the DUMP parameter. The values listed are the extended traces that are currently active.

System action

None.

User response

None.

System programmer response

None.

200-: Active server traces - *value_1 value_2 ... value_n*

Explanation

The SITE command was specified with the DEBUG parameter. The values listed are the general traces that are currently active.

System action

None.

User response

None.

System programmer response

None.

200-: BLOCKSIZE being set to *blksize*

Explanation

The SIte subcommand was entered with one or more of the LRECL, RECFM, and BLKSIZE parameters, and the resulting parameter values caused a mismatch between the LRECL, RECFM, and BLKSIZE parameters. The BLKSIZE value is reset to a compatible value, *blksize*.

System action

The BLKSIZE parameter is reset to *blksize*.

User response

If necessary, reissue the SIte subcommand with a valid LRECL and RECFM combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: BLOCKSIZE must be a multiple of LRECL for RECFM *recfm*

Explanation

The SIte subcommand was entered with one or more of the LRECL, RECFM, and BLKSIZE parameters, and the resulting parameter values caused a mismatch between the LRECL, RECFM, and BLKSIZE parameters. The Record Format, *recfm*, requires that BLKSIZE be a multiple of LRECL, but the BLKSIZE was not a multiple of LRECL.

System action

FTP attempts to set the parameters to compatible values. This reply is followed by another 200- reply indicating which values have been reset.

User response

If necessary, reissue the SIte subcommand with a valid LRECL, RECFM, and BLKSIZE combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: BLOCKSIZE must be at least 4 more than LRECL for RECFM *recfm*

Explanation

The SIte subcommand was entered with one or more of the LRECL, RECFM, and BLKSIZE parameters, and the resulting parameter values caused a mismatch between the LRECL, RECFM, and BLKSIZE parameters. The Record Format, *recfm*, requires that BLKSIZE be at least 4 more than LRECL, but the BLKSIZE was not at least 4 more than LRECL.

System action

FTP attempts to set the parameters to compatible values. This reply is followed by another 200- reply indicating which values have been reset.

User response

If necessary, reissue the SIte subcommand with a valid LRECL, RECFM, and BLKSIZE combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: BLOCKSIZE must equal LRECL for RECFM *recfm*

Explanation

The SIte subcommand was entered with one or more of the LRECL, RECFM, and BLKSIZE parameters, and the resulting parameter values caused a mismatch between the LRECL, RECFM, and BLKSIZE parameters. The Record Format, *recfm*, requires that LRECL and BLKSIZE be equal, but the values for BLKSIZE and LRECL were not the same.

System action

FTP attempts to set the parameters to compatible values. This reply is followed by another 200- reply indicating which values have been reset.

User response

If necessary, reissue the SIte subcommand with a valid LRECL, RECFM, and BLKSIZE combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Blocksize parameter *(value)* is not numeric. Blocksize ignored.

Explanation

The SITE command was specified with the BLKSIZE parameter, but the value, *value*, specified for the BLKSIZE parameter was not a numeric value. The value for BLKSIZE must be a numeric value between 1 and 32760.

System action

The BLKSIZE parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Blocksize parameter *(value)* must be between 0 and 32760. Blocksize ignored.

Explanation

The SITE command was specified with the BLKSIZE parameter, but the value, *value*, specified for the BLKSIZE parameter was outside the valid range. The value for the BLKSIZE parameter must be a numeric value between 0 and 32760.

System action

The BLKSIZE parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: BUfno parameter *(value)* is not numeric. BUfno ignored.

Explanation

The SITE command was specified with the BUFNO parameter, but the value, *value*, specified for the BUFNO parameter was not a numeric value.

System action

The BUFNO parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: BUfno parameter *(value)* must be between 1 and 255 - BUfno ignored.

Explanation

The SITE command was specified with the BUFNO parameter, but the value, *value*, specified for the BUFNO parameter was outside the valid range.

System action

The BUFNO parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200: BUfno parameter *value* must be from *minimum* to *maximum*. BUfno ignored.

Explanation

The SIte subcommand was specified with the BUFNO parameter, but the value specified for the BUFNO parameter was outside the valid range.

value is the value entered for BUfno.

minimum is the minimum allowed value.

maximum is the maximum allowed value.

System action

The BUFNO parameter is ignored.

User response

Reissue the subcommand with a valid value. See the z/OS Communications Server: IP User's Guide and Commands for information about the parameters of the SIte subcommand.

System programmer response

None.

200 : CCC command successful

Explanation

The FTP server received a CCC command that was processed successfully. The FTP client can send unprotected commands on the control connection.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Chkptint parameter *(value)* is not numeric. Chkptint ignored.

Explanation

The value of the CHKPTInt parameter, *value*, was not a numeric value, or was outside the acceptable range.

System action

The parameter is ignored.

User response

Reissue the SITE command with a valid value specified for the CHKPTInt parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Chkptint parameter *(value)* is larger than a 4 byte integer. Chkptint ignored.

Explanation

The value of the CHKPTInt parameter, *value*, was larger than the maximum value allowed for a 4 byte integer.

System action

The value in error is ignored.

User response

Reissue the SITE command with a valid value specified for the CHKPTInt parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Chmod cannot access file *filename* : *error*

Explanation

The FTP server encountered an error attempting to obtain the file information for *filename*. *error* is the C run-time library error encountered while accessing the file.

System action

The CHMOD parameter is ignored.

User response

Reissue the SITE command with a valid value specified for the file name on the CHMOD parameter. If the problem persists, contact the system programmer.

System programmer response

If necessary, correct the error indicated by *error*.

200-: Chmod failed: *error*

Explanation

The FTP server encountered an error attempting to change the permission bits of the file. *error* is the C run-time library error returned in response to the chmod() request.

System action

The CHMOD parameter is ignored.

User response

Contact the system programmer.

System programmer response

Correct the error indicated by *error*

200-: Chmod filename is not a valid z/OS UNIX file. CHMOD ignored

Explanation

The file name specified on the CHMOD parameter of the SIte subcommand was not a z/OS UNIX file. The CHMOD parameter is valid only for a z/OS UNIX files.

System action

The CHMOD parameter is ignored.

User response

Reissue the SITE command with a valid value specified for the file name on the CHMOD parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Chmod invalid filename *filename*

Explanation

The file name specified by the CHMOD parameter of the SIte subcommand was longer than the z/OS UNIX file name maximum of 1023 characters. If the file name operand of the CHMOD parameter began with a forward slash (/), the *filename* value will be the file name operand used “asis”; otherwise *filename* will be the file name operand appended to the current working directory.

System action

The CHMOD parameter is ignored.

User response

Reissue the SITE command with a valid value specified for the file name on the CHMOD parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Chmod invalid syntax. Specify CHMOD mode filename. CHMOD ignored

Explanation

The Chmod parameter of the SITE command was entered incorrectly. The correct syntax of the CHMOD parameter of the SIte subcommand is SITE CHMOD *mode filename* where *mode* is the new permission bit setting for the file, and *filename* is the name of the file to change.

System action

The CHMOD parameter is ignored.

User response

Reissue the SITE command with the correct syntax for the CHMOD parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Chmod mode value invalid. Specify mode as a 1-3 digit octal value, or as {u|g|o|a}{=|+|-}{r|w|x|rw|rx|wx|rwx}. CHMOD ignored

Explanation

The SITE command was entered with the CHMOD parameter, but the mode operand of the CHMOD parameter was incorrect. The mode operand specifies the permission bit settings of the file, and should be expressed as either a 1-3 digit octal number (for example, 666 for permission setting rw-rw-rw-), or as a mnemonic indicating the changed bits, (for example a+x to turn on the execute bit for user, group, and other).

System action

The CHMOD parameter is ignored.

User response

Re-issue the SIte subcommand, specifying the correct value for the mode operand. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Chmod not allowed when user not logged in. CHMOD ignored.

Explanation

The SIte subcommand was issued with the CHMOD parameter, but the user was not currently logged in to the server with a valid user ID. The user must first log in with a valid user ID and password or password phrase before issuing the SIte subcommand with the CHMODE parameter.

System action

FTP continues.

User response

Log in to the server using the USER and PASS subcommands, then reissue the SIte subcommand with the CHMOD parameter.

System programmer response

200-: Chmod parameters missing. Specify CHMOD mode filename. CHMOD ignored

Explanation

The SITE command was entered with the CHMOD parameter, but the syntax of the CHMOD parameter was incorrect. One or more of the operands required on the CHMOD parameter were missing. The syntax of the CHMOD parameter is SITE CHMOD *mode filename*.

System action

The CHMOD parameter is ignored.

User response

Re-issue the SIte subcommand, specifying the correct operands. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

200-: Conddisp parameter *(value)* is invalid. Conddisp ignored.

Explanation

The SITE command was entered with the CONDDISP parameter, but the value specified, *value*, was not a valid value. Valid values for the CONDDISP parameter are Catlg and Delete.

System action

The CONDDISP parameter is ignored.

User response

Re-issue the SIte subcommand, specifying the correct value for CONDDISP. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Conflicting SITE operands *keyword1* and *keyword2*. *Keyword2* ignored.

Explanation

A SITE command was entered with two keywords that conflict. The second keyword is ignored.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Ctrlconn invalid syntax. Specify CTRLCONN=ascii_code_page_name or CTRLCONN=7BIT. CTRLCONN ignored.

Explanation

A SIte subcommand was entered with a CTRLCONN parameter whose value begins with an opening parenthesis [(]. The syntax for the CTRLCONN parameter does not use parentheses. The CTRLCONN parameter is ignored.

System action

FTP continues.

User response

Reissue the SITE command with corrected syntax.

System programmer response

None.

200 : Data connection protection set to *protection*

Explanation

The FTP server successfully processed a PROT command and returned a reply to indicate the data connection protection level.

protection is clear, safe, or private.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: DATAKEEPALIVE value *value* out of range - value must be 0 or between 60 and 86400 - parameter is ignored

Explanation

The server received a SITE command that specified the DATAKEEPALIVE parameter, but the value specified was not within the expected range. The DATAKEEPALIVE parameter specifies the number of seconds of inactivity before a keepalive packet is sent on the FTP data connection.

In the reply text:

value
The value that was not within the allowed range. The DATAKEEPALIVE value must be in the range 60 - 86400.

Example

```
EZA1701I >>> SITE DATAKEEPALIVE=86401
200-DATAKEEPALIVE value 86401 out of range - value must be 0 or between 60 and 86400 -
parameter is ignored
200 SITE command was accepted
EZA1460I Command: .
```

System action

Processing continues.

User response

Reissue the SIte subcommand that specifies a valid DATAKEEPALIVE value.

See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for information about the parameters of the SIte subcommand.

System programmer response

None.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

200-: Data set "*dsname*" does not exist. Dcbdsn parameter ignored.

Explanation

The SIte subcommand been issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, could not be found.

System action

The DCBDSN parameter is ignored.

User response

Reissue the SITE DCBDSN subcommand, specifying a valid MVS data set.

System programmer response

None.

200-: "*dsname*" invalid dsorg. DCBDSN parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, did not have a valid data set organization, or the FTP server was not able to determine the data set organization of the data set. Only MVS PS and PDS data sets can be used as a model DCB data set by the FTP server.

System action

The DCBDSN parameter is ignored.

User response

Reissue the SITE DCBDSN subcommand, specifying a valid MVS data set.

System programmer response

None.

200-: "*dsname*" is a VSAM data set. Dcbdsn parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, was a Virtual Storage Access Method (VSAM) data set. Only MVS PS and PDS data sets can be used as a model DCB data set by the FTP server.

System action

The DCBDSN parameter is ignored.

User response

Reissue the SITE DCBDSN subcommand, specifying a valid MVS data set.

System programmer response

None.

200-: "*dsname*" is migrated and noautorecall is specified. DCBDSN parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, was migrated and the FTP server could not recall the data set because NOAUTORECALL had been specified at the server.

System action

The DCBDSN parameter is ignored.

User response

Issue the SIte subcommand with the AUTORECALL parameter to allow the data set to be recalled.

System programmer response

None.

200-: "*dsname*" is not on a direct access volume. Dcbdsn parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, was not located on a direct access volume. The model DCB data set must be located on a direct access volume to be used by the FTP server.

System action

The DCBDSN parameter is ignored.

User response

Reissue the SITE DCBDSN subcommand, specifying a valid MVS data set.

System programmer response

None.

200-: Data set name missing from DCBDSN parameter. DCBDSN parameter ignored.

Explanation

The DCBDSN parameter of the SIte subcommand was specified with an equal sign, but no data set name followed the equal sign.

System action

The DCBDSN parameter is ignored. FTP continues.

User response

If the SITE DCBDSN= was issued to setup a model DCB data set, reissue the command specifying a data set after the equal sign. If the SITE DCBDSN= was issued to clear the setting of the model DCB data set, reissue the command with no equal sign. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200: Data transfer is mixed SBCS/DBCS

Explanation

The FTP server received a valid DBCS TYPE command from the client. The current transfer type has now been changed to transmit mixed SBCS/DBCS data.

System action

Program execution continues. The current FTP transfer type now uses mixed SBCS/DBCS data.

User response

None.

System programmer response

None.

200: Data transfer is pure DBCS

Explanation

The FTP server received a valid DBCS TYPE command from the client. The current transfer type has now been changed to transmit only pure DBCS data. No SO/SI characters will be present in EBCDIC DBCS data.

System action

Program execution continues. The current FTP transfer type now treats EBCDIC data as pure DBCS data with no SO/SI characters.

User response

None.

System programmer response

None.

200: Data transfer mode is *type*

Explanation

The MODE command was entered to change the data transfer mode to the type shown. The request is processed successfully.

System action

The data transfer mode is changed. FTP continues.

User response

None.

System programmer response

None.

200-: Dataclass parameter *(value)* is more than 8 characters. Dataclass ignored.

Explanation

The value, *value*, specified for the Dataclass parameter is not valid. The Dataclass parameter value cannot be more than 8 characters long.

System action

The Dataclass parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the DATACLASS parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: DB2 parameter *(db2name)* is more than 4 characters. DB2 ignored.

Explanation

The *db2name* specified for the DB2® parameter on an FTP SITE command is too long.

System action

The DB2 parameter is ignored. FTP continues.

User response

Correct the name of the DB2 subsystem, and send the SITE command again.

System programmer response

None

200-: Debug values not supported :*value_1 value_2 ... value_n*

Explanation

The SITE command was specified with the DEBUG parameter. One or more values that were specified are not supported.

value_1 ... value_n are the values that were specified but are not supported.

System action

The DEBUG parameter values are ignored.

User response

Correct the values that are incorrect.

System programmer response

None.

200-: Dest node longer than 8 characters. Dest ignored.

Explanation

The DEST parameter of the SITE command was specified with a user ID and node, and the node operand was longer than 8 characters. The node operand must be 8 characters or less.

System action

The DEST parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the DEST parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Dest user longer than 8 characters. Dest ignored.

Explanation

The DEST parameter of the SITE command was specified with a user ID and node, and the user ID operand was longer than 8 characters. The user ID operand must be 8 characters or less.

System action

The DEST parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the DEST parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Destination *(value)* is more than 8 characters. Dest ignored.

Explanation

The destination, *value*, specified for the DEST parameter is not valid. The Dest parameter destination operand cannot be more than 8 characters long.

System action

The Dest parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the DEST parameter.

System programmer response

None.

200-: Directory parameter *(value)* is not numeric. Directory ignored.

Explanation

The SITE command was specified with the DIRECTORY parameter, but the value, *value*, specified for the DIRECTORY parameter was not a numeric value.

System action

The DIRECTORY parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Directory parameter *(value)* must be between 1 and 16777215. Directory ignored.

Explanation

The SITE command was specified with the DIRECTORY parameter, but the value, *value*, specified for the DIRECTORY parameter was outside the valid range.

System action

The DIRECTORY parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Dump values not supported -*value_1 value_2 ... value_n*

Explanation

The SITE command was specified with the DUMP parameter. One or more values that were specified are not supported.

value_1 ... value_n are the values that were specified but are not supported.

System action

The DUMP parameter values are ignored.

User response

Correct the values that are incorrect.

System programmer response

None.

200: EPRT request OK

Explanation

The client sent an EPRT command to the server. The server accepted the EPRT command. The FTP server will connect its next data socket to the IP address and port number specified on the EPRT command.

System action

FTP continues.

User response

None.

System programmer response

None.

200: EPSV ALL accepted

Explanation

The client sent an EPSV ALL command to the server. The server accepted the EPSV ALL command.

System action

For the rest of the current FTP login session, the server will accept EPSV commands on this session, but reject PASV, PORT, and EPRT commands.

User response

If you need to use PASV, PORT, or EPRT commands, exit the current session and log in to the FTP server again.

System programmer response

None.

200-: Error locating file "*dsname*". DCBDSN parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The FTP server was unable to locate the data set, *dsname*, which was specified as the model DCB data set.

System action

The DCBDSN parameter is ignored.

User response

Reissue the SITE DCBDSN subcommand, specifying a valid MVS data set.

System programmer response

None.

200-: Error mounting "*dsname*". DCBDSN parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, was on a volume that was not mounted to the system, and the FTP server encountered an error attempting to have the volume mounted.

System action

The DCBDSN parameter is ignored.

User response

Contact the system programmer

System programmer response

Determine why the volume cannot be mounted and correct the error.

200-: Error retrieving "*dsname*". DCBDSN parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, was migrated, and the FTP server encountered an error attempting to retrieve the data set.

System action

The DCBDSN parameter is ignored.

User response

Contact the system programmer

System programmer response

Determine why the data set cannot be recalled and correct the error.

200-: Filename for Xlate parameter (*name*) exceeds maximum length of *length*. Xlate ignored.

Explanation

A SIte subcommand was entered with an Xlate=*name* parameter. The corresponding environment variable defines a fully qualified file name that is too long for FTP to use for a translate table file for the data connection. The Xlate parameter is ignored.

System action

FTP continues.

User response

If *name* is correct, contact the system programmer for the FTP server.

System programmer response

Ensure that the fully qualified file name specified by the _FTPXLATE_*name* environment variable is not longer than *length* characters. If FTP tracing was active, there will be a trace entry displaying actual length and the first *length* characters of the file name defined by the environment variable for the Xlate parameter *name*.

200-: Filetype parameter *(value)* is invalid. Filetype ignored.

Explanation

The value, *value*, specified for the FILETYPE parameter is not valid. FILETYPE must be SEQ, JES, or SQL.

System action

The FILETYPE parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the FILETYPE parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Ignoring *parameter*. The keyword was already specified on this SITE command.

Explanation

The keyword specified on the SITE command was already encountered on this SITE command. A parameter can only be issued once per SITE command. All occurrences of the parameter after the first occurrence are ignored.

System action

The keyword is set to the value specified the first time the parameter was encountered.

User response

If you wish to change the parameter to a specification that was not the first one on the SITE command, reissue the SITE command with the appropriate parameters.

System programmer response

None.

200-: Ignoring *parameter=value*. The keyword was already specified on this SITE command.

Explanation

parameter=value was specified on the SITE command, but the keyword was already encountered on this SITE command. A parameter can only be issued once per SITE command. All occurrences of the parameter after the first occurrence are ignored.

System action

parameter is set to the value specified the first time the parameter was encountered.

User response

If you wish to change the parameter value to the value specified by *parameter=value*, reissue the SITE command with *parameter=value* as the only occurrence of the parameter on the SITE command.

System programmer response

None.

200-: Invalid format data set name "*name*". Dcbdsn parameter ignored.

Explanation

The data set name specified for the DCBDSN parameter of the SITE command, which is used to specify the name of the data set to be used as a model for allocation of new data sets, has an incorrect format. The data set name must conform to MVS data set naming conventions.

System action

The DCBDSN parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid MVS data set name. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Invalid record format '*value*' encountered.

Explanation

The SIte subcommand encountered an invalid internal value for the record format.

System action

FTP attempts to reset the BLKSIZE, RECFM, and LRECL parameter values back to the default values.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

200-: JESINTERFACELEVEL=*value*. The value of *keyword* cannot be modified.

Explanation

The keyword specified can only be modified when JESINTERFACELEVEL=2.

System action

The SITE parameter is ignored. FTP continues.

User response

Ensure that the JESINTERFACELEVEL=2 and reissue the SITE command.

System programmer response

None.

200-: Jeslrecl parameter *(value)* is not numeric. Jeslrecl ignored.

Explanation

The SITE command was specified with the JESLRECL parameter, but the value, *value*, specified for the JESLRECL parameter was not a numeric value. The value for the JESLRECL parameter must be a numeric value in the range 1–254, or an asterisk (*).

System action

The JESLRECL parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: JesLrecl parameter must be between 1 and 254. JesLrecl parameter ignored.

Explanation

The value submitted for the JESLRECL parameter, which is used to specify the logical record length for the JES internal reader at the remote host, was not within the valid range of 1 through 254.

System action

The JESLRECL parameter is ignored. FTP continues.

User response

Reissue the SITE command specifying value for the JESLRECL parameter in the valid range of 1 to 254. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Jesrecfm parameter *(parameter)* is invalid. Jesrecfm ignored.

Explanation

The value specified for the record format of the Job Entry Subsystem (JES) internal reader, JESRECFM, is not a valid value for that parameter. JESRECFM must be F, V, or *.

System action

The JESRECFM value is ignored. FTP continues.

User response

Reissue the SITE command specifying a valid value for JESRECFM. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: *keyword*=*value* ignored. Unable to set up requested conversion.

Explanation

A CTRLCONN parameter was entered on a SIte subcommand, but FTP was unable to build the single-byte translate tables for the control connection. The CTRLCONN parameter is ignored. The translate tables for the control connection are not changed.

Note: If the FTP server is running in a double-byte environment, the CTRLCONN parameter cannot be used to change the translate tables for the control connection.

System action

FTP continues.

User response

None.

System programmer response

If the FTP server is running in a double-byte code set, the CTRLCONN parameter is not supported. The tables used for the control connection are set at server initialization from either a TCPXLBIN file, or from FTP's internal default single-byte tables.

If the server is running in a single-byte environment, an internal error occurred. If this occurs repeatedly, contact the IBM Support Center with an FTP trace.

200: Language is en-US (United States English)

Explanation

The FTP server received a LANG command requesting English or one of its variations as the language to use for server replies. The server will use United States English for server replies. See RFC 2640 for more information about the LANG command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

Processing continues.

User response

None.

System programmer response

None.

200- : Language reverts to default en-US (United States English)

Explanation

The server received a LANG command with no arguments. The server has reverted to its default language for FTP server replies. See RFC 2640 for more information about the LANG command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

Processing continues.

User response

None.

System programmer response

None.

200: Load module transfer reset

Explanation

Load module transfer processing was aborted because it was not required. The transfer operation continues using normal processing.

System action

FTP continues.

User response

None.

System programmer response

None.

200: Local byte size is 8, representation type is Image

Explanation

The FTP TYPE L command was accepted, and the data transfer type is set to Image.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: LRECL being changed to *lrecl*

Explanation

The SIte subcommand was entered with one or more of the LRECL, RECFM, and BLKSIZE parameters, and the resulting parameter values caused a mismatch between the LRECL, RECFM, and BLKSIZE parameters. The LRECL value is changed to a compatible value, *lrecl*.

System action

The LRECL parameter is reset to *lrecl*.

User response

If necessary, reissue the SIte subcommand with a valid LRECL, RECFM, and BLKSIZE combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: LRECL being reset to *lrecl*.

Explanation

The SIte subcommand was entered with one or more of the BLKSIZE, LRECL, and RECFM parameters, and the resulting parameter values were incompatible The LRECL value is reset to a compatible value, *lrecl*.

System action

The LRECL parameter is reset to the value it had prior to the SIte subcommand, if compatible, otherwise it is reset to the value from FTP.DATA, if compatible, otherwise it is set to the default.

User response

Reissue the SIte subcommand with a valid LRECL, RECFM, and BLKSIZE combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: LRECL being reset to SITE default of ‘not used’.

Explanation

The SIte subcommand was entered with one or more of the LRECL, RECFM, and BLKSIZE parameters, and the resulting parameter values were incompatible. The previous LRECL value was also not compatible and the LRECL was reset to the value specified in the FTP.DATA file. The value in the FTP.DATA file was a NULL value, indicating that the LRECL should be unspecified.

System action

The LRECL parameter is reset to the NULL value from the FTP.DATA file.

User response

If necessary, reissue the SIte subcommand with a valid BLKSIZE, LRECL, and RECFM combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Lrecl parameter *(value)* is not numeric. Lrecl ignored.

Explanation

The SITE command was specified with the LRECL parameter, but the value, *value*, specified for the LRECL parameter was not a numeric value. The value for the LRECL parameter must be a numeric value between 0 and 32760.

System action

The LRECL parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Lrecl parameter *(value)* must be between 0 and 32760. Lrecl ignored.

Explanation

The SITE command was specified with the LRECL parameter, but the value, *value*, specified for the LRECL parameter was outside the valid range. The value for the LRECL parameter must be a numeric value between 0 and 32760.

System action

The LRECL parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: LRECL X valid only for RECFM of U or variable length spanned.

Explanation

The SIte subcommand was entered with the LRECL and/or RECFM parameters, and the resulting parameter values caused a mismatch between the LRECL and RECFM parameters. The LRECL value was X, but the RECFM was not U or variable length spanned. Logical record length of X is only valid when the record format is U, VS, VSA, VSM, VBS, VBSA, or VBSM.

System action

FTP attempts to reset the values to compatible values. This reply is followed by another 200- reply indicating which values have been reset.

User response

Reissue the SIte subcommand with a valid LRECL and RECFM combination. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: LRECL 0 valid only for RECFM of U.

Explanation

The SIte subcommand was entered with the LRECL and/or RECFM parameters, and the resulting parameter values caused a mismatch between the LRECL and RECFM parameters. The LRECL value was 0, but the RECFM was not U. Logical record length of 0 is only valid when the record format is U.

System action

FTP attempts to set the parameters to compatible values. This reply is followed by another 200- reply indicating which values have been reset.

User response

If necessary, reissue the SIte subcommand with a valid LRECL and RECFM combination. See the z/OS Communications Server: IP User's Guide and Commands, in the informationabout transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: LRECL, RECFM, and BLOCKSIZE being reset to default values.

Explanation

The SITE command encountered an unresolvable incompatibility between the RECFM, LRECL and BLKSIZE parameter values and has reset all three parameter values back to the default.

System action

FTP attempts to reset the BLKSIZE, RECFM, and LRECL parameter values back to the default values.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

200-: Mgmtclass parameter *(value)* is more than 8 characters. Mgmtclass ignored.

Explanation

The value, *value*, specified for the Mgmtclass parameter is not valid. The Mgmtclass parameter value cannot be more than 8 characters long.

System action

The Mgmtclass parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the MGMTCLASS parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Migratevol parameter *(value)* is more than 6 characters. Migratevol ignored.

Explanation

The value, *value*, specified for the Migratevol parameter is not valid. The Migratevol parameter value cannot be more than 6 characters long.

System action

The Migratevol parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the MIGRATEVOL parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: NCP parameter not supported for the C server. NCP ignored.

Explanation

The SITE command was entered with the NCP parameter, but the NCP parameter is not supported for the FTP C server.

System action

The NCP parameter is ignored. FTP continues.

User response

None.

System programmer response

None.

200-: No conversion available to *'cp_name1'* from *'cp_name2'*. MBDATACONN ignored.

Explanation

A SITE command was entered with the MBDATACONN parameter, but there is no supported code set converter for the code sets that are specified. The MBDATACONN parameter is ignored.

cp_name1 is the codepage name to which the code is converted.

cp_name2 is the codepage name from which the code is converted.

System action

FTP continues.

User response

See the z/OS XL C/C++ Programming Guide for information about supported code set converters and valid code set names. Reissue the corrected SITE command.

System programmer response

None.

200-: No conversion available between *parm1* and *parm2*. SBDATACONN ignored.

Explanation

A SIte subcommand was entered with an SBDATACONN parameter, but there is no supported code set converter for the code sets *parm1* and *parm2*. The SBDATACONN parameter is ignored.

System action

FTP continues.

User response

See the z/OS XL C/C++ Programming Guide for information about supported code set converters and valid code set names. Reissue the corrected SIte subcommand, with the EBCDIC code set name as the first SBDATACONN value, followed by the ASCII code set name.

System programmer response

None.

200-: No storage volumes exist.

Explanation

The QDISK parameter was entered without a specific volume serial number. When this parameter is left blank, statistics about all storage volumes are displayed. No storage volumes were found.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: No users are allowed to use SITE DEBUG

Explanation

The SITE command was specified with the DEBUG parameter. The FTP server does not allow users to change the debug (general tracing) options with the SITE command.

System action

The DEBUG parameter is ignored.

User response

If the system programmer changes the FTP server as stated below, the user must establish a new FTP session after the server is restarted before issuing SITE DEBUG.

System programmer response

If users are to be allowed to change the debug options with the SITE command, add the DEBUGONSITE TRUE statement to the FTP server's FTP.DATA file and restart the FTP server.

200-: No users are allowed to use SITE DUMP

Explanation

The SITE command was specified with the DUMP parameter. The FTP server does not allow users to change the dump (extended tracing) options with the SITE command.

System action

The DUMP parameter is ignored.

User response

If the system programmer changes the FTP server as stated below, the user must establish a new FTP session after the server is restarted before issuing SITE DUMP.

System programmer response

If users are to be allowed to change the dump options with the SITE command, add the DUMPONSITE TRUE statement to the FTP server's FTP.DATA file and restart the FTP server.

200-: Nowrtapefastio ignored. Wrtapefastio already specified on this Site command.

Explanation

The WRTAPEFastio parameter was already specified on this SITE command. The NOWRTAPEFastio parameter is ignored.

System action

FTP continues.

User response

Issue the SITE command again with the desired setting.

System programmer response

None.

200: OK

Explanation

A NOOP command was executed successfully, indicating that the remote host is still responding. For more information about the NOOP command, see the z/OS Communications Server: IP User's Guide and Commands or type HELP NOOP on the command line.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Operand not allowed on *parm* parameter. Parameter ignored.

Explanation

The parameter *parm* appeared on a SITE command in incorrect format. No operand is allowed for this parameter. The parameter is ignored.

System action

FTP continues.

User response

If desired, reissue the SITE command without an operand on the *parm* parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: operand required on *parm* parameter. Parameter ignored.

Explanation

The parameter *parm* appeared on a SITE command without an operand. The parameter is ignored.

System action

FTP continues.

User response

If desired, reissue the SITE command with an operand for the *parm* parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Parameter *keyword* value *value* is not numeric - the parameter is ignored

Explanation

A value that is not numeric was specified for a SIte subcommand parameter. The parameter assignment is ignored.

In the reply text:

keyword
The parameter that was specified.

value
The non-numeric value that was specified.

Example

```
EZA1701I >>> SITE DATAKEEPALIVE=Ab
200-Parameter DATAKEEPALIVE value Ab is not numeric - the parameter is ignored
200 SITE command was accepted
EZA1460I Command: .
```

System action

The specified parameter is ignored and processing continues.

User response

Reissue the SIte subcommand with a valid value for the specified parameter.

See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for information about the parameters of the SIte subcommand.

System programmer response

None.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

200-: Parameter *parameter* value *value* must be in the range *minimum* to *maximum* - parameter is ignored

Explanation

A value was specified for a SITE command parameter that is outside of the expected range. The parameter assignment was ignored.

In the reply text:

parameter
The parameter specified on the SIte subcommand.

value
The value entered for the SITE parameter.

minimum
The minimum allowed value.

maximum
The maximum allowed value.

Example

```
site DSWAITTIME=14401
 EZA1701I >>> SITE DSWAITTIME=14401
 200-Parameter DSWAITTIME value 14401 must be between 0 and 14400 - parameter is
ignored
 200 SITE command was accepted
 EZA1460I Command:
```

System action

The parameter is ignored and processing continues.

User response

Reissue the SITE command with a valid value for the specified parameter.

See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for information about the parameters of the SIte subcommand.

System programmer response

None.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

200-: *parameter=operand* ignored. Requested conversion is not supported.

Explanation

A CTRLCONN paramter was entered on a SIte subcommand, but there is no conversion available between the FTP server's code page and *operand*. The CTRLCONN parameter is ignored. The translate tables for the control connection are not changed.

System action

FTP continues.

User response

Reissue the SITE command, specifying either "7bit" or the name of an ASCII code page supported by iconv. See the z/OS XL C/C++ Programming Guide for a list of the code pages supported by iconv. The code page name must be entered exactly as shown in the list (for example: IBM-850 or ISO8859-1).

System programmer response

None

200 : PBSZ=0 is the protection buffer size

Explanation

The FTP server received a command to set the Protection Buffer Size (PBSZ) to a nonzero value. The connection is protected by the TLS security mechanism, which does not accept a PBSZ value greater than 0. The PBSZ command completed successfully but the PBSZ is set to 0.

System action

FTP continues.

User response

None.

System programmer response

None

200 : PBSZ=*size*

Explanation

The client used a PBSZ command to request a maximum size for protected buffers sent on the data connection. The FTP server set the size to a value less than or equal to the client's requested size.

size is the negotiated maximum size of protected buffers sent on the data connection.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Percent Free Free Largest Free

Explanation

The server received a SITE command with the QDISK parameter specified. The QDISK parameter requests space information for one or more volumes on the FTP server host. This reply is the first line of a header for a group of replies that the server sends to report space statistics for one or more volumes.

See reply code “200-: volume percent_free free_cylinders free_tracks largest_cyls largest_trks free_extents use_attribute” on page 515 for more information.

Example

```
site qdisk=vtamfv
CR1165 site: entered
>>> SITE qdisk=vtamfv
200-        Percent      Free      Free          Largest    Free
200- Volume Free         Cyls      Trks         Cyls-Trks   Exts  Use Attr
200- VTAMFV    3           64        71           20    0     32  Private
200 SITE command was accepted
Command:

>>> SITE qdisk
200-        Percent      Free      Free          Largest    Free
200- Volume Free         Cyls      Trks         Cyls-Trks   Exts  Use Attr
200- CPDLB3   58         1937       112         1523    0  99999+ Storage
200- CPDLB4   77         2570        76         2190    0     16  Storage
200- CPDLB0   44          486       158          461    0     26  Storage
200- CPDLB1    1            0       316            0   20     54  Storage
200 SITE command was accepted
Command:
```

System action

Processing continues.

User response

None.

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

200: Port request OK.

Explanation

The PORT command was accepted.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Primary parameter *(value)* is not numeric. Primary ignored.

Explanation

The SITE command was specified with the PRIMARY parameter, but the value, *value*, specified for the PRIMARY parameter was not a numeric value.

System action

The PRIMARY parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Primary parameter *(value)* must be between 1 and 16777215. Primary ignored.

Explanation

The SITE command was specified with the PRIMARY parameter, but the value, *value*, specified for the PRIMARY parameter was outside the valid range.

System action

The PRIMARY parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200 : Protection buffer size accepted

Explanation

The FTP server received a command to set the Protection Buffer Size (PBSZ) to 0. The request was accepted.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Qdisk ignored. "*value*" is not a valid volser.

Explanation

The value, *value*, specified for the QDISK parameter was not a valid volume serial name. The value specified for QDISK must be 6 characters or less.

System action

The QDISK parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the QDISK parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Qdisk workarea allocation failed.

Explanation

The allocation of the workarea for qdisk failed. number.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: READTAPEFormat *value* is not supported - READTAPEFormat ignored

Explanation

The value specified for the READTAPEFormat parameter on a SITE command is not supported.

value can be one of the following values:

- F (for fixed)
- V (for variable)
- S (for spanned)
- X (for lrecl X)
- blank (unspecified)

System action

The READTAPEFormat parameter is ignored. FTP continues.

User response

Change *value* to one of the supported formats.

System programmer response

None.

200-: Recfm parameter *(value)* is invalid. Recfm ignored.

Explanation

The value, *value*, specified for the record format is invalid. The record format must be one of: F, FA, FB, FBA, FBM, FBS, FM, V, VA, VB, VBA, VBM, VBS, VM$, VS, U, or blank.

System action

The RECFM value is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the RECFM parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Representation type is Big5

Explanation

The FTP server received a valid TYPE B 8 command from the FTP client. The current transfer type has successfully been changed to Big5.

System action

Program execution continues. The current FTP transfer type is changed.

User response

None.

System programmer response

None.

200: Representation type is Ebcdic IBM Kanji

Explanation

The FTP TYPE F command was accepted, and the data transfer type is the IBM kanji code, which is based on the EBCDIC code set.

System action

FTP continues.

User response

None.

System programmer response

None.

200: Representation type is Image

Explanation

The FTP TYPE I command was accepted, and the data transfer type is image (or binary). With the image transfer type, data is sent as continuous bits, packed into 8-bit bytes.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Representation type is SChinese

Explanation

The FTP server received a valid TYPE B 9 command from the FTP client. The current transfer type has successfully been changed to Simplified Chinese.

System action

Program execution continues. The current FTP transfer type is changed.

User response

None.

System programmer response

None.

200: Representation type is *type*

Explanation

The FTP server received a valid TYPE subcommand, and the data representation type was changed.

System action

FTP continues.

User response

None.

System programmer response

None.

200: Representation type is UCS-2

Explanation

The FTP server received a valid TYPE U 2 command from the FTP client. The current transfer type has successfully been changed to UCS-2.

System action

Program execution continues. The current FTP transfer type is changed.

User response

None.

System programmer response

None.

200-: Retpd parameter *(value)* is not numeric. Retpd ignored.

Explanation

The SITE command was specified with the RETPD parameter, but the value, *value*, specified for the RETPD parameter was not a numeric value. The value specified for the RETPD parameter must be a numeric value between 0 and 9999.

System action

The RETPD parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Retpd parameter *(value)* must be between 0 and 9999. Retpd ignored.

Explanation

The SITE command was specified with the RETPD parameter, but the value, *value*, specified for the RETPD parameter was outside the valid range. The value of RETPD must be a numeric value between 0 and 9999.

System action

The RETPD parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Sbdataconn invalid syntax. Specify SBDATACONN=(value1,value2) or SBDATACONN=dsn. SBDATACONN ignored.

Explanation

A SIte subcommand was issued with a SBDATACONN parameter that has an incorrect syntax. The SBDATACONN parameter must be either a pair of code set names (the first must be an EBCDIC code set name, and the second must be an ASCII code set name), or the fully qualified name of an MVS data set or z/OS UNIX file containing translate tables generated by the CONVXLAT utility.

System action

FTP continues.

User response

Issue the SIte subcommand with corrected syntax.

System programmer response

None.

200-: Sbdataconn parameter is too long. Maximum length for code page name is *length*. SBDATACONN ignored.

Explanation

A SIte subcommand was entered with an SBDATACONN parameter specifying a invalid code page name. The SBDATACONN parameter is ignored.

System action

FTP continues.

User response

See the z/OS XL C/C++ Programming Guide for information on supported code set converters and valid code set names. Reissue the corrected SIte subcommand.

System programmer response

None.

200-: SBSUBChar parameter (*sbsubchar*) is not valid - SBSUBChar ignored

Explanation

The value of the SBSUBChar parameter must be either a hexadecimal number or SPACE.

sbsubchar is not a valid substitution character.

System action

The parameter is ignored.

User response

Reissue the SITE command with a valid value specified for the SBSUBChar parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol, for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Secondary parameter *(value)* is not numeric. Secondary ignored.

Explanation

The SITE command was specified with the SECONDARY parameter, but the value, *value*, specified for the SECONDARY parameter was not a numeric value.

System action

The SECONDARY parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Secondary parameter *(value)* must be between 0 and 16777215. Secondary ignored.

Explanation

The SITE command was specified with the SECONDARY parameter, but the value, *value*, specified for the SECONDARY parameter was outside the valid range.

System action

The SECONDARY parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200: SITE command was accepted

Explanation

The SIte subcommand was accepted and processed. If an error was detected in any SIte subcommand parameters, this reply will be preceded by one or more 200- replies indicating any parameter errors.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Some characters cannot be translated between *codeset_1* and *codeset_2*

Explanation

The SITE SBDATACONN command specified the code set names for the file system code set and the network transfer code set. The iconv() function was used to build a table for each of the 256 single character codepoints. Some of the codepoints do not have an equivalent codepoint. If FTP detects a data byte during the transfer of the data that cannot be translated using the tables, the data transfer will fail.

codeset_1 is the name of the file system code set.

codeset_2 is the name of the network transfer code set.

System action

The tables are built and will be used during data transfer by FTP.

User response

Specify SITE SBDATACONN with code set names that convert all of the codepoints. However, you can use the table if your data does not contain any of the untranslatable characters.

System programmer response

To see which of the codepoints cannot be translated, start the server with the following trace specified in the FTP.DATA file:

```
DEBUG UTL         ; utility services trace
```

200-: SO/SI characters *char* used

Explanation

The FTP server received a valid DBCS TYPE command from the client. The current transfer type now includes the use of SO/SI characters shown to delimit ASCII DBCS data.

System action

Program execution continues.

User response

None.

System programmer response

None.

200-: Sqlcol parameter *(value)* is invalid. Sqlcol ignored.

Explanation

The value submitted for the SQLCOL parameter, which is used to determine the column headings of the output file, was not valid. Valid values for the SQLCOL parameter are:

Type
Description

Names
Uses the names of the Db2® SQL table columns. The labels are ignored.

Labels
Uses the labels of the SQL table columns. If any of the columns do not have labels, the corresponding column heading in the output file is given a heading of 'COLnnn'

Any
The label of the Db2 SQL table column is the first choice for column heading in the output file. If there is no label, the column name is used.

System action

The SQLCOL parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the SQLCOL parameter. See the information about the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands .

System programmer response

None.

200: Standard DBCS control used

Explanation

The FTP server received a valid DBCS TYPE command from the client. Standard DBCS control will be used. For JIS78KJ and JIS83KJ the selected escape sequences are used and for all other ASCII types no SO/SI characters are used. Data transfer is also set to mixed SBCS/DBCS.

System action

Program execution continues. The current FTP transfer type is changed.

User response

None.

System programmer response

None.

200-: Storclass parameter *(value)* is more than 8 characters. Storclass ignored.

Explanation

The value, *value*, specified for the Storclass parameter is not valid. The Storclass parameter value cannot be more than 8 characters long.

System action

The Storclass parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the STORCLASS parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: SUBSYS parameter *(value)* is more than 4 characters - SUBSYS parameter is ignored

Explanation

The server received a SITE command that specified a SUBSYS parameter that is too long. The SUBSYS parameter cannot be longer than 4 characters.

In the reply text:

value
The value that you specified for the SUBSYS parameter.

Example

```
EZA1701I >>> SITE SUBSYS=F1234
200-SUBSYS parameter F1234 is more than 4 characters - SUBSYS parameter is ignored.
200 SITE command was accepted
```

System action

The parameter is ignored and processing continues.

Operator response

Not applicable.

User response

Reissue the SITE command with a valid value for the specified parameter. If the client is a z/OS FTP client, see the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for information about the SUBSYS parameter.

System programmer response

Not applicable.

Problem determination

Not applicable.

Source

Not applicable.

Module

Not applicable.

Routing code

Not applicable.

Descriptor code

Not applicable.

200-: The keyword *keyword* value of *value* is not valid. Parameter ignored.

Explanation

The value specified for the keyword is not valid. Valid values for JESSTATUS are ACTIVE, INPUT, OUTPUT, and ALL. Valid values for JESENTRYLIMIT are whole numbers between 1 and 1024. Valid values for JESINTERFACELEVEL are 1 and 2. Valid values for JESOWNER and JESJOBNAME are a character string that can include the asterisk (*) and question mark (?) wildcards.

System action

The parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the parameter. See the information about the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands .

System programmer response

None.

200: Transferring PDS directory information.

Explanation

PDS directory information will be transmitted along with the PDS member.

System action

None.

User response

None.

System programmer response

None.

200-: Translate file '*file*' invalid. SBDATACONN ignored.

Explanation

A SIte subcommand was entered with an SBDATACONN parameter that specified a file name, but FTP encountered an error while trying to load its translate tables using *file*. Possible errors include an invalid header record or incorrect file length. (The file must contain exactly 768 bytes of data.) The SBDATACONN parameter is ignored.

System action

FTP continues.

User response

Ensure that the file name specified is correct. It must be a fully qualified name, and the file must contain translate tables in the format generated by the CONVXLAT utility.

System programmer response

If FTP tracing was active, an EZY message will appear in FTP's system log and trace output explaining why FTP cannot use the file.

200-: Translate file '*file*' not found. SBDATACONN ignored.

Explanation

A SIte subcommand was entered with an SBDATACONN parameter that specified a file name, but FTP was unable open *file*. The SBDATACONN parameter is ignored.

System action

FTP continues.

User response

Ensure that the file name specified on the SBDATACONN parameter is a fully qualified name of an existing MVS data set or z/OS UNIX file.

System programmer response

If the file name is correct, look in the FTP server's trace for the reason why FTP cannot open the file.

200-: Translate file for Xlate name '*name*' not found. Xlate ignored.

Explanation

A SIte subcommand was entered with an Xlate parameter to specify a translate table file but FTP was unable to find or open a file for that Xlate name. The Xlate parameter is ignored.

System action

FTP continues.

User response

If the name provided was correct, contact the system programmer for the FTP server.

System programmer response

Ensure that a binary translate table file exists as hlq.*name*.TCPXLBIN, or if you wish to use a file with a different name, ensure that an environment variable was set at FTP server start to specify the different name. The environment variable must be called _FTPXLATE_*name*, the environment variable name must be all uppercase, and the environment variable must be set to a fully qualified file name. The FTP server's trace will contain the environment variables that were defined when the server was started. It will also contain the name of the file that FTP tried to open in response to the SITE command and the reason why the file could not be opened.

200-: Translate file for Xlate name '*name*' not valid. Xlate ignored.

Explanation

A SIte subcommand was entered with an Xlate parameter, but FTP encountered an error while trying to load translate tables from the file indicated by *name*. Possible errors include an invalid header record or incorrect file length. (The file must contain exactly 768 bytes of data.) The Xlate parameter is ignored.

System action

FTP continues.

User response

If *name* is correct, contact the system programmer for the FTP server.

System programmer response

Ensure that hlq.*name*TCPXLBIN, or the file specified by the _FTPXLATE_*name* environment variable, contains translate tables in the format generated by the CONVXLAT utility. If FTP tracing was active, an EZY message will appear in FTP's system log and trace output explaining why FTP cannot use the file.

200-: UCOUNT parameter *(value)* is neither numeric, nor P. UCOUNT ignored.

Explanation

The value of the UCOUNT parameter, *value*, was not a numeric value, nor was it the letter P.

System action

The parameter is ignored.

User response

Reissue the SITE command with a valid value specified for the UCOUNT parameter. See the z/OS Communications Server: IP User's Guide and Commands for information on the parameters of the SIte subcommand.

System programmer response

None.

200-: UCOUNT parameter *(value)* must be between 1 and 59, or P. UCOUNT ignored.

Explanation

The SITE command was specified with the UCOUNT parameter, but the value, *value*, specified for the UCOUNT parameter was outside the valid numeric range.

System action

The UCOUNT parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands for information on the parameters of the SIte subcommand.

System programmer response

None.

200-: Umask invalid syntax. Specify UMASK umask_value. UMASK ignored

Explanation

The SITE command was issued with the UMASK parameter, but the syntax of the UMASK parameter was incorrect. The correct syntax is SITE UMASK *umask_value*, where *umask_value* is a 3 character octal number representing file permission bits.

System action

The UMASK parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the UMASK parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Umask value invalid. Specify Umask value as 1 - 3 octal digits

Explanation

The SITE command was issued with the UMASK parameter, but the value specified for the UMASK parameter was invalid. The value specified for UMASK should be a 1 to 3 character octal number representing file permission bits.

System action

The UMASK parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the UMASK parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Umask value missing. Specify Umask value as 1 - 3 octal digits

Explanation

The SITE command was issued with the UMASK parameter, but no value was specified for the UMASK parameter. The value specified for UMASK should be a 1 to 3 character octal number representing file permission bits.

System action

The UMASK parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the UMASK parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Unable to set up conversion between '*parm1*' and '*parm2*'. SBDATACONN ignored.

Explanation

A SIte subcommand was entered with an SBDATACONN parameter. A code set convertor was successfully opened, but FTP was unable to set up single-byte translate tables using the requested code sets. The SBDATACONN parameter is ignored.

System action

FTP continues.

User response

Ensure that the requested code set names are for single-byte code pages. SBDATACONN is not supported for double-byte. See the z/OS XL C/C++ Programming Guide for information on supported code set converters and valid code set names.

System programmer response

None.

200-: Unable to set up conversion between UCS-2 and *codeset*

Explanation

The FTP server was unable to setup a conversion between UCS-2 and EBCDIC or EBCDIC and UCS-2 when SITE UCSHOSTCS was received.

System action

UCSHOSTCS is ignored.

User response

If you want to change the UCSHOSTCS value, reissue the SITE UCSHOSTCS command to change the EBCDIC code set. For information about UCSHOSTCS, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

200-: Unit ignored. "*value*" is not a valid unit parameter.

Explanation

The value, *value*, specified for the UNIT parameter was not a valid unit name. The value specified for UNIT must be 8 characters or less.

System action

The Unit parameter is ignored. FTP continues.

User response

Reissue the SITE command with a valid value for the UNIT parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Unrecognized parameter '*parameter*=*operand*' on SITE command.

Explanation

The SIte subcommand was entered with the parameter *parameter*, but *parameter* was not a valid SIte subcommand parameter.

System action

The parameter is ignored. FTP continues.

User response

Reissue the SIte subcommand with a valid parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: Unrecognized parameter '*parameter*' on SITE command.

Explanation

The SIte subcommand was entered with the parameter *parameter*, but *parameter* was not a valid SIte subcommand parameter.

System action

The parameter is ignored. FTP continues.

User response

Reissue the SIte subcommand with a valid parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: User *userid* is not authorized to filter on *keyword*. Its value remains *value*.

Explanation

The user ID must have SAF READ access to SDSF resource ISFCMD.FILTER.OWNER to change JESOWNER.

To change JESJOBNAME, the user ID must have SAF READ access to SDSF resource ISFCMD.FILTER.PREFIX.

The user ID must have SAF READ access to SDSF resource ISFCMD.DSP.INPUT.jesx, ISFCMD.DSP.ACTIVE.jesx, and ISFCMD.DSP.OUTPUT.jesx to set JESSTATUS to INPUT, ACTIVE, and OUTPUT, respectively. READ access to all three is required to set JESSTATUS to ALL. If the user ID has no access to the three ISFCMD.DSP.** SDSF resources the user ID will not be able to change JESOWNER, JESJOBNAME or JESSTATUS from their default values.

System action

The SITE parameter is ignored. FTP continues.

User response

Ensure that the user has the proper SAF resource access.

System programmer response

None.

200-: User *user_name* is not allowed to use SITE DEBUG

Explanation

The SITE command was specified with the DEBUG parameter. *user_name* is not permitted to change the debug (general tracing) options with the SITE command because the user is not allowed access by the server's security product.

System action

The DEBUG parameter is ignored.

User response

Try again after your user ID is added to the resource class.

System programmer response

If the user is allowed to change debug options with the SITE command, permit the user to access the profile defined by the security product. See the z/OS Communications Server: IP Diagnosis Guide for information about Start Tracing after FTP initialization, the SERVAUTH class, and the profile that restricts the use of the SITE DEBUG command.

200-: User *user_name* is not allowed to use SITE DUMP

Explanation

The SITE command was specified with the DUMP parameter. The user is not permitted to change the dump (extended tracing) options with the SITE command because he is not allowed access by the server's security product.

System action

The DUMP parameter is ignored.

User response

Try again after your user ID is added to the resource class.

System programmer response

If the user is allowed to change debug options with the SITE command, permit the user to access the profile defined by the security product. See the z/OS Communications Server: IP Diagnosis Guide for information about Start Tracing after FTP initialization, the SERVAUTH class, and the profile that restricts the use of the SITE DEBUG command.

200-: VCOUNT parameter is not numeric. VCOUNT ignored.

Explanation

The value of the VCOUNT parameter, *value*, was not a numeric value.

System action

The parameter is ignored.

User response

Reissue the SITE command with a valid value specified for the VCOUNT parameter. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using the file transfer protocol for information about the parameters of the SIte subcommand.

System programmer response

None.

200-: VCOUNT parameter must be between 1 and 255. VCOUNT ignored.

Explanation

The SITE command was specified with the VCOUNT parameter, but the value, *value*, specified for the VCOUNT parameter was outside the valid range.

System action

The VCOUNT parameter is ignored.

User response

Reissue the command with a valid value. See the z/OS Communications Server: IP User's Guide and Commands for information on the parameters of the SIte subcommand.

System programmer response

None.

200-: volume for "*dsname*" is not mounted and noautomount is specified. DCBDSN parameter ignored.

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, was on a volume that was not mounted to the system and the FTP server could not mount the volume because NOAUTOMOUNT had been specified at the server.

System action

The DCBDSN parameter is ignored.

User response

Issue the SIte subcommand with the AUTOMOUNT parameter to allow the volume to be mounted.

System programmer response

None.

200-: Volume Free Cyls Trks Cyls-Trks Exts Use Attr

Explanation

The server received a SITE command with the QDISK parameter specified. The QDISK parameter requests space information for one or more volumes on the FTP server host. This reply is the second line of a header for a group of replies that the server sends to report space statistics for one or more volumes.

See reply code "200-: volume percent_free free_cylinders free_tracks largest_cyls largest_trks free_extents use_attribute" on page 515 for more information.

Example

```
site qdisk=vtamfv
CR1165 site: entered
```

```
>>> SITE qdisk=vtamfv
200-        Percent      Free      Free          Largest    Free
200- Volume Free         Cyls      Trks         Cyls-Trks   Exts  Use Attr
200- VTAMFV    3           64        71           20    0     32  Private
200 SITE command was accepted
Command:

>>> SITE qdisk
200-        Percent      Free      Free          Largest    Free
200- Volume Free         Cyls      Trks         Cyls-Trks   Exts  Use Attr
200- CPDLB3   58         1937       112         1523    0  99999+ Storage
200- CPDLB4   77         2570        76         2190    0     16  Storage
200- CPDLB0   44          486       158          461    0     26  Storage
200- CPDLB1    1            0       316            0   20     54  Storage
200 SITE command was accepted
Command:
```

System action

FTP continues.

User response

None.

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

200-: Volume ignored. “*value*” is not a valid volume parameter

Explanation

The server detected a syntax error in the value, *value*, specified for the SITE VOLUME command. The value specified for VOLUME must be a volume serial number or a list of volume serial numbers.

System action

The Volume parameter is ignored. FTP continues.

User response

Issue the SITE command with a valid value for the VOLUME parameter. See the z/OS Communications Server: IP User's Guide and Commands for information on the syntax of the SITE VOLUME subcommand.

System programmer response

None.

200-: *volume percent_free free_cylinders free_tracks largest_cyls largest_trks free_extents use_attribute*

Explanation

The server received a SITE command with the QDISK parameter specified. The QDISK parameter requests space information for one or more volumes on the FTP server host. This reply is one of a group of replies the server sends to report space statistics for one or more volumes.

In the message text:

volume
The volume serial number of a volume on the FTP server host.

percent_free
The percent of free space on the volume identified by the *volume* value.

free_cylinders
The number of free cylinders on the volume identified by the *volume* value.

free_tracks
The number of free tracks on the volume identified by the *volume* value.

largest_cyls
The number of cylinders in the largest free extent on the volume identified by the *volume* value.

largest_trks
The number of tracks in the largest free extent on the volume identified by the *volume* value.

free_extents
The number of free extents on the volume identified by the *volume* value. If the number of free extents exceeds 99 999, the value 99999+ is displayed.

use_attribute
The use attribute of the volume identified by the *volume* value.

Example

```
 >>> SITE qdisk=vtamfv
200-        Percent      Free      Free          Largest    Free
200- Volume Free         Cyls      Trks         Cyls-Trks   Exts  Use Attr
200- VTAMFV    3           64        71           20    0     32  Private
200 SITE command was accepted
Command:


>>> SITE qdisk
200-        Percent      Free      Free          Largest    Free
200- Volume Free         Cyls      Trks         Cyls-Trks   Exts  Use Attr
200- CPDLB3   58         1937       112         1523    0  99999+ Storage
200- CPDLB4   77         2570        76         2190    0     16  Storage
200- CPDLB0   44          486       158          461    0     26  Storage
200- CPDLB1    1            0       316            0   20     54  Storage
200 SITE command was accepted
Command:
```

System action

No action is needed.

User response

No action is needed.

System programmer response

No action is needed.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

200-: Volume *volser* could not be found.

Explanation

The QDISK parameter was entered with volume serial number *volser*. The requested volume serial number could not be found.

System action

FTP continues.

User response

None.

System programmer response

None.

200-: Waiting for mount for "*dsname*"

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, is on a volume that is not mounted to the system. The volume must first be mounted to the system.

System action

FTP waits for the volume for *dsname* to be mounted, then continues processing the DCBDSN parameter of the SIte subcommand.

User response

None.

System programmer response

None.

200-: Waiting for recall of "*dsname*"

Explanation

The SIte subcommand was issued with the DCBDSN parameter. The data set specified as the model DCB, *dsname*, is migrated and must be recalled.

System action

FTP waits for *dsname* to be recalled, then continues processing the DCBDSN parameter of the SIte subcommand.

User response

None.

System programmer response

None.

200-: Wrtapefastio ignored. Nowrtapefastio already specified on this Site command.

Explanation

The NOWRTAPEFastio parameter was already specified on this SIte subcommand. The WRTAPEFastio parameter is ignored.

System action

FTP continues.

User response

Issue the SIte subcommand again with the desired setting.

System programmer response

None.

200-: Xlate parameter (*xlate_name*) is more than 8 characters. Xlate ignored.

Explanation

xlate_name exceeds the maximum length of 8 characters.

System action

Xlate is ignored.

User response

If you wish to use the Xlate parameter, reissue the command specifying an xlate_name that is no more than 8 characters long.

System programmer response

None.

202 reply codes

202: ACCT command not required - ignored

Explanation

The FTP server received the ACCT command, which is not supported under MVS. The command is ignored.

System action

FTP continues.

User response

Use the USER command instead of the ACCT command. For more information about the USER command, see the z/OS Communications Server: IP User's Guide and Commands, or type HELP USER at the command line.

System programmer response

None.

202: ALLO not necessary, you may proceed

Explanation

The FTP server received the ALLO command, which is not supported under MVS. The command is ignored.

System action

FTP continues.

User response

None.

System programmer response

None.

202: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command is in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

202: SITE not necessary; you may proceed

Explanation

The SIte subcommand was entered with no parameters.

System action

FTP continues.

User response

None.

System programmer response

None.

205 reply codes

205: Load module transfer syntax error

Explanation

An unexpected or incorrectly formatted load module transfer command was sent to the server. This is a violation of the load module transfer protocol.

System action

Load module transfer processing is aborted and the file transfer is completed using base processing. Any MVS Load modules transferred will not be executable on the target system.

User response

Contact your system programmer.

System programmer response

Ensure that the server and client are both Communications Server for z/OS. If they are not, contact the vendor of the non-IBM FTP program for service.

205: Load module transfer syntax error: blksize parameter missing.

Explanation

The blocksize parameter was missing from an XLMT DCB command. This is a violation of the load module transfer protocol.

System action

Load module transfer processing is aborted and the file transfer is completed using base processing. Any MVS Load modules transferred will not be executable on the target system.

User response

Contact your system programmer.

System programmer response

Ensure that the server and client are both Communications Server for z/OS. If they are not, contact the vendor of the non-IBM FTP program for service.

205: Load module transfer syntax error: lrecl parameter missing.

Explanation

The logical record length parameter was missing from an XLMT DCB command. This is a violation of the load module transfer protocol.

System action

Load module transfer processing is aborted and the file transfer is completed using base processing. Any MVS Load modules transferred will not be executable on the target system.

User response

Contact your system programmer.

System programmer response

Ensure that the server and client are both Communications Server for z/OS. If they are not, contact the vendor of the non-IBM FTP program for service.

211 reply codes

211: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The subcommand in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

211-: Confidence level in data transfers is neither checked nor reported

Explanation

This message is displayed as part of the STAT subcommand output when the statement CHKCONFIDENCE is set to FALSE.

System action

Processing continues.

User response

If you want to activate confidence checking and reporting, see the CHKCONFIDENCE statement in z/OS Communications Server: IP Configuration Reference for more information about coding the CHKCONFIDENCE statement in FTP.DATA.

System programmer response

None.

211-: Confidence level in data transfers is checked and reported

Explanation

This message is part of the STAT reply. It means that the confidence level in successful completion of data transfers in the FTP server will be determined and reported in FTP log message EZYFS86I. The CHKCONFIDENCE TRUE FTP.DATA statement sets this condition. Message EZYFS86I is issued when FTPLOGGING is active.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: Confidence level in data transfers is not checked or reported

Explanation

This message is part of the STAT reply. It means that the confidence level in successful completion of a data transfer in the FTP server will not be determined or reported in FTP log message EZYFS86I. This does not disable error reporting. The CHKCONFIDENCE FALSE FTP.DATA statement sets this condition.

System action

FTP continues.

User response

None.

System programmer response

None.

Module

EZAFTPRT

Destination

ftpstat

211-: DBSUB is set to *dbsub*

Explanation

DBSUB can be set to either TRUE or FALSE.

dbsub is one of the following values:

TRUE
Indicates that a substitution character is used when untranslatable characters are encountered during the data transfer.

FALSE
Indicates that the data transfer will fail when an untranslatable character is encountered during file transfer. FALSE is the default setting.

The DBSUB value is set by coding the DBSUB statement in FTP.DATA, or by using the SIte subcommand with the DBSUB or NODBSUB parameter. See the description of the DBSUB statement in z/OS Communications Server: IP Configuration Reference for more information about coding the DBSUB statement. See the information about the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information about the DBSUB and NODBSUB parameters.

System action

FTP continues.

User response

None.

System programmer response

None.

Module

EZAFTPRT

Destination

ftpstat()

211: End

Explanation

The server sent a 211- message to the client in response to a FEAT command. This message signals the end of the current message. See RFC 2389 for more information about the FEAT command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

Processing continues.

User response

None.

System programmer response

None.

211-: Extensions supported

Explanation

The server received a FEAT command from the client. This reply code is followed immediately by a list of features or extensions supported by the server. See RFC 2389 for more information about the FEAT command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

Processing continues.

User response

None.

System programmer response

None.

211-: ISPFSTATS is set to *ispfstats*

Explanation

ISPFSTATS can be set to either TRUE or FALSE. When ISPFSTATS is set to TRUE, ISPF Statistics of a PDS member that was transferred to the FTP client will be updated or created. The default setting is FALSE.

ispfstats is either TRUE or FALSE.

System action

FTP Continues.

User response

None.

System programmer response

None.

211: no Extensions supported

Explanation

The server received a FEAT command from the client. The server supports no features or extensions with an architected FEAT response. See RFC 2389 for more information about the FEAT command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

Processing continues.

User response

None.

System programmer response

None.

211-: Outbound MBCS ASCII data uses *lt_chars* line terminator

Explanation

This reply is issued in response to the STAT command. Each line of multi-byte data being transferred to the client and translated to ASCII in the FTP server will use the displayed line terminator. This value is determined by the SITE command MBSENDEOL parameter or the MBSENDEOL FTP.DATA statement.

lt_chars is the line terminator that will be used. Values for *lt_chars* are:

CRLF
Multi-byte data translated to ASCII will use the combination of a carriage return (x'0D') and line feed (x'0A') to terminate each line. This is the default and the standard line terminator defined by RFC 959. The z/OS server and client can receive ASCII data only in this format.

CR
Multi-byte data translated to ASCII will use only a carriage return (x'0D') to terminate each line.

LF
Multi-byte data translated to ASCII will use only a line feed (x'0A') to terminate each line.

NONE
Multi-byte data translated to ASCII will use no line terminator characters.

System action

FTP continues.

User response

Change the setting, if necessary, with the SITE command MBSENDEOL parameter or MBSENDEOL FTP.DATA statement.

System programmer response

None.

211-: Outbound SBCS ASCII data uses *lt_chars* line terminator

Explanation

This reply is issued in response to the STAT command. Each line of single-byte data being transferred to the client and translated to ASCII in the FTP server will use the displayed line terminator. This value is determined by the SITE command SBSENDEOL parameter or the SBSENDEOL FTP.DATA statement.

lt_chars is the line terminator that will be used. Values for *lt_chars* are:

CRLF
Single-byte data translated to ASCII will use the combination of a carriage return (x'0D') and line feed (x'0A') to terminate each line. This is the default and the standard line terminator defined by RFC 959. The z/OS server and client can receive ASCII data only in this format.

CR
Single-byte data translated to ASCII will use only a carriage return (x'0D') to terminate each line.

LF
Single-byte data translated to ASCII will use only a line feed (x'0A') to terminate each line.

NONE
Single-byte data translated to ASCII will use no line terminator characters.

System action

FTP continues.

User response

Change the setting with the SITE command SBSENDEOL parameter or SBSENDEOL FTP.DATA statement if necessary.

System programmer response

None.

211-: Partitioned data sets will be created in extended format.

Explanation

This reply is used only when DIRECTORY is defined and PDSTYPE is set to PDSE. See the z/OS Communications Server: IP Configuration Reference for information about the DIRECTORY and PDSTYPE statements in FTP.DATA. See the z/OS Communications Server: IP User's Guide and Commands for information about the DIRECTORY and PDSTYPE parameters of the SIte subcommand.

System action

Processing continues.

User response

None.

System programmer response

None.

211-: Records on input tape are fixed format

Explanation

This message is part of the STAT reply. It means that a value of F was specified for READTAPEFormat and the record format for an input tape is expected to be fixed. This value must be consistent with the tape label when the data set is opened.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: Records on input tape are lrecl X format

Explanation

This message is part of the STAT reply. It means that a value of X was specified for READTAPEFormat and the record format for an input tape is expected to be lrecl X. This value must be consistent with the tape label when the data set is opened.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: Records on input tape are spanned format

Explanation

This message is part of the STAT reply. It means that a value of S was specified for READTAPEFormat and the record format for an input tape is expected to be spanned. This value must be consistent with the tape label when the data set is opened.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: Records on input tape are unspecified format

Explanation

This message is part of the STAT reply. It means that no value was specified for READTAPEFormat and the record format for an input tape will not be known until the data set is opened.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: Records on input tape are variable format

Explanation

This message is part of the STAT reply. It means that a value of V was specified for READTAPEFormat and the record format for an input tape is expected to be variable. This value must be consistent with the tape label when the data set is opened.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: SBSUBCHAR is set to *sbsubchar*

Explanation

During the file transfer, untranslatable codepoints will be replaced by the substitution character *sbsubchar*. This setting is ignored if SBSUB is set to FALSE. If SPACE is specified, the ASCII or EBCDIC representation of a blank will be substituted.

sbsubchar is either a SPACE or a substitution in hexadecimal.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: SBSUB is set to *sbsub*

Explanation

SBSUB can be set to either TRUE or FALSE.

sbsub is one of the following values:

TRUE
Indicates that a substitution character is used when untranslatable characters are encountered during the data transfer.

FALSE
Indicates that the data transfer will fail when an untranslatable character is encountered during file transfer. FALSE is the default setting.

System action

FTP continues.

User response

None.

System programmer response

None.

211-: Server site variable *statement_name* is set to *value*

Explanation

This message is displayed as part of the STAT command reply.

statement_name is the name of the statement coded in the server FTP.DATA file.

value is the current setting of *statement_name*. It is the default value assigned by FTP, the value that you specified in the FTP.DATA file, or the most recent value that you assigned with a **site** command to the server.

System action

Processing continues

User response

If you want to change the setting of *statement_name* temporarily, use the **site** subcommand. See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information.

If your FTP client is z/OS, you can use the **site** subcommand to change *value* temporarily.

System programmer response

If you want to make a permanent change to *statement_name*, see the z/OS Communications Server: IP Configuration Reference for information about coding the statement specified by *statement_name*.

211-: Timer *timer_name* is set to *timer_value*

Explanation

This reply is part of the server STAT command response. It indicates the current setting for a timer used by FTP.

timer_name is the name of the timer as coded in FTP.DATA . See the z/OS Communications Server: IP Configuration Reference for a description of the FTP.DATA *timer_name* statement.

timer_value is the current setting of *timer_name*.

System action

Processing continues.

User response

None.

System programmer response

None.

211: The value of option *option* is undefined

Explanation

This reply is issued in response to the XSTA command and indicates that the value of the specified option is undefined.

option is the option specified on the XSTA command

System action

FTP continues.

User response

None.

System programmer response

None.

211: TLS security is supported at the *tlsRfcLevel* level

Explanation

This reply is part of the server STAT command response. This reply indicates the level of RFC 4217 that is supported by the z/OS server.

In the reply text:

tlsRfcLevel
The level of support as coded with the TLSRFCLEVEL statement in the server's FTP.DATA file. See the FTP.DATA TLSRFCLEVEL statement in z/OS Communications Server: IP Configuration Reference for a description of the FTP.DATA TLSRFCLEVEL statement.

Example

```
211-TLS security is supported at the DRAFT level
```

System action

Processing continues.

User response

None.

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

211-: UTF-8 encoding in use on the control connection

Explanation

The server received a STAT command from the client. This part of the STAT reply indicates that the server is currently using UTF-8 encoding for the control connection. See RFC 2640 for more information about UTF-8 encoding. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

Processing continues.

User response

If you do not want to use UTF-8 encoding for the control connection, issue the SITE CTRLCONN and LOCSITE CTRLCONN subcommands to change the control connection encoding. See the z/OS Communications Server: IP User's Guide and Commands for more information about the SITE and LOCSIte subcommands.

System programmer response

If you do not want the server to use or accept UTF-8 encoding on the control connection, remove the EXTENSIONS UTF8 statement from the server's FTP.DATA file. See the z/OS Communications Server: IP Configuration Reference for more information about the EXTENSIONS statement.

213 reply codes

213: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

213: Status: *number* bytes transferred

Explanation

The STAT command was received as an Out Of Band command during data transfer. When the STAT command is received during data transfer, the server returns only the number of bytes transferred on the data connection.

System action

FTP continues.

User response

None.

System programmer response

None.

213: YYYYMMDDHHMMSS

Explanation

The MDTM command was issued to the FTP Server for a certain path name. This response indicates when the path name was last modified, according to the Gregorian calendar.

YYYY
is the year;

MM
is a number from 1 to 12 indicating the month;

DD
is a number from 1 to 31 indicating day of the month;

HH
is a number from 0 to 23 indicating hour of the day;

MM
is a number from 0 to 59 indicating minute of the hour;

ss
is a number from 0 to 61 indicating second of the minute, values 60 and 61 implying leap seconds.

System action

FTP continues.

User response

None.

System programmer response

None.

214 reply codes

214: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

214: XDSS *dsname*: extract the attributes of an MVS data set.

Explanation

Reply to HELP server xdss.

Example

```
help server xdss
EZA1701I >>> HELP XDSS
EZA1582I The foreign server has this help:
214 XDSS dsname: extract the attributes of an MVS data set.
```

System action

No action is needed.

Operator response

No action is needed.

User response

No action is needed.

System programmer response

No action is needed.

214-: READTAPEFormat=value Format of input tape data sets. Valid formats are

Explanation

Reply to HELP SITE.

214-: F (for fixed), V (for variable), S (for spanned),

Explanation

Reply to HELP SITE.

214-: X (for lrecl X), and blank (unspecified).

Explanation

Reply to HELP SITE.

215 reply codes

215: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

215: MVS is the operating system of this server. FTP Server is running on *name*.

Explanation

The FTP server handling the file transfer uses the MVS operating system. This is the FTP server that runs under z/OS UNIX System Services and is capable of handling z/OS UNIX files.

name is the name of the operating system.

System action

FTP continues.

User response

None.

System programmer response

None.

215: UNIX is the operating system of this server. FTP Server is running on *name*.

Explanation

The FTP server handling the file transfer uses the UNIX System Services operating system. This is the FTP server that runs under z/OS System Services and is capable of handling z/OS UNIX files.

name is the name of the operating system.

System action

FTP continues.

User response

None.

System programmer response

None.

220 reply codes

220: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

220: Connection will close if idle for more than *timeout*

Explanation

The FTP server was started with a timeout value of *timeout*. If there is no activity on the control connection between the client and the server for the specified amount of time, the control connection will end.

Note: The inactivity timer is not in effect during data transfer. The inactivity timer is only in effect during the time between the successful completion of one subcommand and the issuing of the next subcommand.

Note: The inactivity timer is for the control connection only. It has no effect on the data connection.

System action

FTP continues.

User response

None.

System programmer response

None.

220: Connection will not timeout.

Explanation

The FTP server was started with no control connection timeout value. The control connection between the client and the server will stay active indefinitely, regardless of whether or not there is activity on the connection.

System action

FTP continues.

User response

None.

System programmer response

None.

220-: FTP *init_time* on *init_date*.

Explanation

The FTP client has successfully contacted the FTP server. The FTP was initiated at *init_time* on *init_date*.

System action

FTP continues.

User response

None.

System programmer response

None.

220-: *jobname* IBM FTP *version_release* at *hostname*, *init_time* on *init_date*.

Explanation

The FTP client successfully contacted the FTP server. The FTP server is at host *hostname*. The FTP server job, *jobname*, was initiated at *init_time* on *init_date*.

System action

FTP continues.

User response

None.

System programmer response

None.

220: Reinitialized; Ready for new user.

Explanation

The FTP server is reinitialized and ready for a new user.

System action

The FTP server is reinitialized and waits for a new user.

User response

None.

System programmer response

None.

220-: The message was truncated.

Explanation

The FTP server banner message exceeded 100 lines. FTP server displays only the first 100 lines of the banner message.

System action

The FTP continues.

User response

Report the error to the system programmer.

System programmer response

Redesign the FTP banner message so it does not exceed 100 lines.

221 reply codes

221: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

221: Quit command received. Goodbye.

Explanation

The Quit command was received. The FTP session and the connection to the host ends.

System action

The FTP session ends.

User response

None.

System programmer response

None.

226 reply codes

226: Abort successful.

Explanation

The ABORT command was received and processed successfully.

System action

If a command is in progress, the command in progress ends. If a data transfer is in progress, the data transfer ends and the data connection is closed. If no command is in progress, no action is taken. The control connection remains active, and the FTP server waits for the next command from the client.

User response

None.

System programmer response

None.

226: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

226-: Compression reduced bytes transferred by *percentage* percent

Explanation

Data is being transferred while in mode c (compressed). The compression algorithm has reduced the number of bytes of data that are transferred for the request by the percentage specified by the *percentage* value.

System action

FTP continues.

User response

None.

System programmer response

None.

226-: DBCS conversion to EBCDIC encountered invalid input (*number* errors)

Explanation

While converting mixed or pure DBCS data to EBCDIC, the server encountered input that is not valid such as a data byte that is not within the valid byte range.

number is the number of errors encountered in the source file.

System action

FTP continues.

User response

Check the source data and correct any errors. Resubmit the data transfer request.

System programmer response

None.

226-: It is known to JES as *job_ID*

Explanation

This reply displays the job ID assigned by the Job Entry System (JES). Use this job ID to access the job through the JES. If the specified job ID is ***UNKNOWN**, the retrieval of the job identifier from JES failed.

System action

FTP continues.

User response

None.

System programmer response

None.

226: List completed successfully.

Explanation

A LIST command was successfully completed.

System action

FTP continues.

User response

None.

System programmer response

None.

226: Nlst completed successfully

Explanation

A command was issued to obtain an NLST file listing. The NLST command completed successfully.

System action

FTP continues.

User response

None.

System programmer response

None.

226-: One or more characters were substituted during the transfer

Explanation

During a single-byte data transfer, one or more untranslatable characters were found and were replaced by the substitution character.

The substitution character is specified by the SBSUBCHAR configuration option; substitution is enabled by the SBSUB configuration option. You can display the current SBSUB and SBSUBCHAR settings by sending a STAT command to the server.

See the SBSUB FTP.DATA statement and SBSUBCHAR FTP.DATA statement in z/OS Communications Server: IP Configuration Reference for more information.

See the SBSUB and SBSUBCHAR options of the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information.

See the STATUS subcommand in z/OS Communications Server: IP User's Guide and Commands for more information.

System action

FTP continues.

User response

If substitution is acceptable, and the current SBSUBCHAR setting is acceptable, no action is needed. Otherwise, issue the SIte subcommand from the z/OS FTP client to change the current settings, and transfer the file again.

Tip: If your client is not the z/OS FTP client, you can use the QUOTE subcommand to send a SITE command to the server.

System programmer response

None.

226: Statistics have been updated for the PDS member that was transferred

Explanation

Statistics had to be updated for the PDS member that was transferred because the PDS member that it replaced had statistics. ISPFSTATS setting of FALSE was ignored.

System action

FTP continues.

User response

None.

System programmer response

None.

226: Transfer completed (data was truncated)

Explanation

A store request or a request to submit a job contains data with a record length that is longer than the record length of the destination data set. Some of the data was truncated (lost).

System action

FTP continues

User response

Specify a logical record length for the destination data set that is big enough for the largest record that is transferred.

System programmer response

None.

226: Transfer completed (lines were wrapped)

Explanation

A store request or a request to submit a job contains data with a record length that is longer than the record length of the destination data set. However, because the WRAPRECORD option is in effect, the data is wrapped into the next record instead of being truncated (lost).

System action

FTP continues.

User response

None.

System programmer response

None.

226: Transfer completed (*number* translation errors)

Explanation

A data transfer request (retrieve or store) or a request to submit a job contains data that must the translated to or from a double-byte character set. The number translation errors that occurred during the translation process is specified by *number*.

System action

FTP continues.

User response

None.

System programmer response

None.

226: Transfer completed successfully.

Explanation

The requested data transfer command successfully completed.

System action

FTP continues.

User response

None.

System programmer response

None.

226: Transfer completed successfully, warning SELECT file too large

Explanation

An SQL query was submitted through FTP. The length of the SQL statement in the input file exceeded 32 765 characters. The SQL statement was truncated to 32 765 characters and submitted to Db2.

System action

FTP continues.

User response

Check the input file used to submit the query. If necessary, correct the SQL statement in the input file, and resubmit the query.

System programmer response

None.

226-: Unicode to EBCDIC conversion resulted in *number* substitutions

Explanation

The requested data transfer command completed. The number of Unicode characters that could not be converted to the EBCDIC code page is specified by the *number* value. Those characters were replaced with the EBCDIC substitution character.

Substitution is allowed by the current UCSSUB setting. If substitution had not been allowed, the file transfer would have failed.

See the UCSSUB statement in z/OS Communications Server: IP Configuration Reference for more information about the UCSSUB statement in FTP.DATA file. See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for information about using the SIte subcommand to change the UCSSUB setting.

System action

FTP continues.

User response

None.

System programmer response

None.

227 reply codes

227: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

227: Entering Passive Mode *(h1,h2,h3,h4,p1,p2)*

Explanation

The server received the PASV subcommand. The server successfully entered passive mode and is listening on the socket indicated by *h1,h2,h3,h4,p1,p2*, where *h1-h4* are the host IP address and *p1,p2* are the port number.

System action

FTP creates the server socket and listens on that socket.

User response

None.

System programmer response

None.

229 reply codes

229: Entering Extended Passive Mode (|||*port_number*|)

Explanation

The server received the EPSV command. The server successfully opened a data socket, and is listening on the socket. The IP address associated with the listening socket is the same as the IP address used for the control connection.

port_number is the port number associated with the listening data socket.

System action

The FTP server continues processing commands on the control connection. The server expects the client to create a data socket and connect it to the IP address of the control connection and port number indicated in the EPSV reply.

User response

None.

System programmer response

None.

230 reply codes

230: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

230-: Password was changed.

Explanation

The PASS command was entered in the format PASS old_pass/new_pass/new_pass to change the password or password phrase during login. The user's password or password phrase was changed. The user can no longer log on to the system using the old password or password phrase.

System action

The user's password or password phrase is changed. FTP continues.

User response

None.

System programmer response

None.

230-: Processing FTPS.RC configuration file - *filename*

Explanation

The FTPS.RC user-level configuration file was found and opened for read access. The FTP server will parse and execute each line.

filename is the FTPS.RC user-level configuration file.

See the z/OS Communications Server: IP User's Guide and Commands for more information about the user-level configuration file.

System action

FTP continues.

User response

None.

System programmer response

None.

230: The email address entered is in an incorrect format.

Explanation

The anonymous user entered a bad email address, but the user is still allowed to log in successfully.

System action

FTP continues.

User response

None.

System programmer response

None.

230-: The message was truncated.

Explanation

The FTP server banner message exceeded 100 lines and was truncated.

System action

The FTP continues.

User response

Report the error to the system programmer.

System programmer response

Redesign the FTP server banner message so that it does not exceed 100 lines.

230-: Unable to open FTPS.RC configuration file - *filename* - *errno*

Explanation

The FTPS.RC user-level configuration file was located, but could not be opened for read access.

filename is the FTPS.RC user-level configuration file.

errno is the decimal z/OS UNIX Return Code. These Return Codes are listed and described in the z/OS UNIX System Services Messages and Codes. The *errno* provides information about why the file could not be opened. A common problem is that the file name permission settings are incorrect.

System action

FTP continues.

User response

Contact the system programmer with the error.

System programmer response

Correct the problem indicated by *errno*. If the problem is caused by incorrect permission bits, use the CHMOD command to change the permission settings of *filename*.

230-: Unrecognized command - *cmd* - entered

Explanation

The user-level configuration file contains a command that is not recognized. The command must be CD, CWD or SITE. The command is ignored.

cmd is the command that was not recognized.

System action

The command was ignored. FTP continues.

User response

Correct the error in the user-level configuration file. If the problem persists, contact the system programmer with the error.

System programmer response

Correct the error in the user-level configuration file. See the z/OS Communications Server: IP User's Guide and Commands for more information about setting user-level options using FTPS.RC.

230: *user_id* is logged on. Working directory is "*directory*".

Explanation

The named user successfully logged on.

System action

FTP continues.

User response

None.

System programmer response

None.

230-: User *userid* is an authorized user

Explanation

The USER command was received specifying the same username that was received during authentication negotiation. The username is authorized and no password or password phrase is required. The client is logged in as *userid*.

userid is the user ID received from the client on the USER command

System action

FTP continues.

User response

None.

System programmer response

None.

230-: Unrecognized parameter '*parameter=operand*'on SITE command.

Explanation

The user-level configuration file contains a SITE command with a parameter or operand that is not recognized.

parameter is the SITE command parameter.

operand is the parameter operand.

System action

The parameter is ignored. FTP continues.

User response

Notify the system programmer.

System programmer response

Correct the error in the user-level configuration file. See the z/OS Communications Server: IP User's Guide and Commands for more information about setting user-level options using FTPS.RC.

234 reply codes

234 : Security environment established - ready for negotiation

Explanation

This reply is in response to the AUTH command. The FTP server is willing to accept the security mechanism specified on the command.

System action

FTP continues.

User response

None.

System programmer response

None.

235 reply codes

235 : ADAT=*base64EncodedData*

Explanation

The client connected to the server using GSSAPI authentication and sent an ADAT command. The server must send an ADAT reply containing the authentication data. The server does not require another ADAT command from the client.

base64EncodedData is the server's authentication data.

System action

FTP continues.

User response

None.

System programmer response

None.

235 : GSSAPI Authentication succeeded

Explanation

The client connected to the server and GSSAPI authentication was successfully negotiated.

System action

FTP continues.

User response

None.

System programmer response

None.

250 reply codes

250: Cancel successful

Explanation

A job submitted through the Job Entry Subsystem (JES) was canceled due to user request.

System action

The job is canceled. FTP continues.

User response

None.

System programmer response

None.

250: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

250-: Compression reduced bytes transferred by *percentage* percent

Explanation

Data is being transferred while in mode c (compressed). The compression algorithm has reduced the number of bytes of data that are transferred for the request by the percentage shown in by *percentage*.

System action

FTP continues.

User response

None.

System programmer response

None.

250: *dsname* deleted.

Explanation

The indicated data set was deleted by user request.

System action

The data set is deleted. FTP continues.

User response

None.

System programmer response

None.

250: *dsname* deleted from migration volume.

Explanation

The data set is migrated and was deleted from the migration volume. Note that if the migration and recall facility is currently inactive, the actual delete might occur later when the facility is activated.

System action

FTP continues.

User response

None.

System programmer response

None.

250: Data structure is File

Explanation

The STRU subcommand was received by the FTP server requesting that the file structure for data transfer be set to FILE. The server processed the command and changed the file structure to FILE.

System action

The File structure is changed to FILE structure.

User response

None.

System programmer response

None.

250: Data structure is Record

Explanation

The STRU subcommand was received by the FTP server requesting that the file structure for data transfer be set to RECORD. The server processed the command and changed the file structure to RECORD.

System action

The file structure is set to RECORD structure

User response

None.

System programmer response

None.

250-: DBCS conversion to EBCDIC encountered invalid input (*number* errors)

Explanation

While converting mixed or pure DBCS data to EBCDIC, the server encountered invalid input such as a data byte that is not within the valid byte range.

System action

FTP continues.

User response

Check the source data and correct any errors. Resubmit the data transfer request.

System programmer response

None.

250: DCB saved, send next command for load module transfer

Explanation

The DCB parameters required for the temporary data set have been saved.

System action

FTP continues.

User response

None.

System programmer response

None.

250: "*directory*" is the working directory name prefix.

Explanation

A CWD command was issued that caused the current working directory of the server to be changed to the MVS high level qualifier *directory*.

System action

FTP continues.

User response

None.

System programmer response

None.

250: directory remains "*old_directory*".

Explanation

A CWD subcommand was entered to change the current working directory, but the FTP server was unable to successfully change the directory. The directory remains unchanged from the old directory.

System action

The directory is unchanged. FTP continues.

User response

This reply is accompanied by other replies that indicate the problem. Correct the errors indicated by the other replies.

System programmer response

None.

250-: Error mounting “*dsname*”;

Explanation

A CWD command was issued to change the current working directory to *dsname*. *dsname* was an existing MVS data set that was catalogued on an unmounted volume. The FTP server needed to mount the volume for the data set in order to determine whether or not the data set was a partitioned data set. The mount of the volume for *dsname* failed. The server was unable to complete the CWD command.

System action

The server attempts to mount the data set, but the mount is unsuccessful. The current working directory is not changed.

User response

Contact the system programmer.

System programmer response

Determine why the mount of the volume failed and correct the problem.

250-: Error retrieving "*dsname*";

Explanation

A CWD command was issued to change the current working directory to *dsname data set* was an existing MVS data set that was migrated. The FTP server needed to recall the data set in order to determine whether or not the data set was a partitioned data set. The recall of migrated data set *dsname* failed.

System action

The server attempts to recall the data set, but the recall is unsuccessful. The current working directory is not changed.

User response

Contact the system programmer.

System programmer response

Determine why the recall of the migrated data set failed and correct the problem.

250: z/OS UNIX directory *directory* is the current working directory

Explanation

The user issued the CWD command to change the current working directory. The CWD command completed successfully and changed the current working directory to a z/OS UNIX directory indicated by *directory*.

System action

The current working directory is changed to the new directory.

User response

None.

System programmer response

None.

250-: It is known to JES as *job_ID*.

Explanation

This reply displays the job ID assigned to a job by the Job Entry System (JES). Use this job ID to access the job through the JES. If the specified job ID is "*UNKNOWN", the retrieval of the job identifier from JES failed.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: JES SSI interface return code *rc*.

Explanation

The Subsystem Interface (SSI) between FTP and JES completed with a non-zero return code. The IEFSSREQ macro completed with the specified decimal value in register 15. The meaning of each value is described in the z/OS MVS Using the Subsystem Interface.

System action

The data transfer ends.

User response

None.

System programmer response

None.

250-: JESENTRYLIMIT of *number* reached. Additional entries not displayed

Explanation

More jobs matched the selection criteria but were not displayed due to the JESENTRYLIMIT value shown.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: JES SSI function *function* SSOBRETN = *rc*

Explanation

An unexpected SSOBRETN value was received from the Subsystem Interface (SSI).

function is the 2-digit SSI function code.

rc is the decimal SSOBRETN return code value.

System action

FTP continues normally.

User response

See the z/OS MVS Using the Subsystem Interface for a description of the SSI function codes and associated return codes (SSOBRETN).

System programmer response

None.

250: List completed successfully.

Explanation

A list command was successfully completed.

System action

FTP continues.

User response

None.

System programmer response

None.

250: Nlst completed successfully

Explanation

A command was issued to obtain a NLST. The NLST command completed successfully.

System action

FTP continues.

User response

None.

System programmer response

None.

250: *old data set* renamed to *new data set*

Explanation

The indicated data set was renamed.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: One or more characters were substituted during the transfer

Explanation

During a data transfer, one or more untranslatable characters were found and were replaced by the substitution character.

You can enable or disable single byte transfer substitution with the SITE command SBSUB and NOSBSUB parameters; or by coding the SBSUB statement in FTP.DATA. You can specify the single byte transfer substitution character with the SITE command SBSUBCHAR parameter, or by coding an SBSUBCHAR statement in FTP.DATA.

You can enable or disable double byte transfer substitution with the SITE command DBSUB and NODBSUB parameters; or by coding the DBSUB statement in FTP.DATA.

See the descriptions of the DBSUB statement, the SBSUB statement, and the SBSUBCHAR statement in z/OS Communications Server: IP Configuration Reference for more information about the DBSUB, SBSUB, and SBSUBCHAR statements in FTP.DATA. See the descriptions of the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information about the DBSUB, SBSUB, and SBSUBCHAR parameters.

System action

FTP continues.

User response

None.

System programmer response

None.

250: Rename requested and the new name is the same as the old.

Explanation

A RENAME was requested and the new file name is the same as the old. The file is not renamed and a normal completion is returned to the client.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: Statistics have been updated for the PDS member that was transferred

Explanation

Statistics had to be updated for the PDS member that was transferred, because the PDS member that it replaced had statistics. ISPFSTATS setting of FALSE was ignored.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: The message was truncated.

Explanation

The FTP server banner message exceeded 100 lines and was truncated.

System action

The FTP continues.

User response

None.

System programmer response

None.

250: The working directory "*directory*" is a partitioned data set

Explanation

A CWD command was issued that caused the current working directory of the server to be changed to the MVS partitioned data set *directory*.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: The working directory might be a load library

Explanation

As a result of the CWD command, the FTP server's working directory is a PDS or a PDSE with RECFM=U. This might be load library, and load module transfer processing might be attempted for this directory.

System action

FTP continues.

User response

None.

System programmer response

None.

250: Transfer completed (data was truncated)

Explanation

A store request or a request to submit a job contains data whose record length is longer than that of the destination data set. Some of the data was truncated (lost).

System action

FTP continues.

User response

Specify a logical record length for the destination data set that is big enough for the largest record that is transferred.

System programmer response

None.

250: Transfer completed (lines were wrapped)

Explanation

A store request or a request to submit a job contains data whose record length is longer than that of the destination data set. However, because the WrapRecord option is in effect, the data is wrapped into the next record instead of being truncated (lost).

System action

FTP continues.

User response

None.

System programmer response

None.

250: Transfer completed (*number* translation errors)

Explanation

A data transfer request (retrieve or store) or a request to submit a job contains data that must the translated to or from a double-byte character set. A total of *number* translation errors occurred during the translation process.

System action

FTP continues.

User response

None.

System programmer response

None.

250: Transfer completed successfully.

Explanation

The requested data transfer command successfully completed.

System action

FTP continues.

User response

None.

System programmer response

None.

250: Transfer completed successfully, warning SELECT file too large

Explanation

A SQL query was submitted through FTP. The length of the SQL statement in the input file exceeded 32765 characters. The SQL statement was truncated to 32765 characters and submitted to Db2.

System action

FTP continues.

User response

Check the input file used to submit the query. If necessary, correct the SQL statement in the input file, and resubmit the query.

System programmer response

None.

250: *type size* - send next command for load module transfer

Explanation

The server is ready to accept the next load module transfer command.

type
The type of load library that the server's current working directory points to (PDS or PDSE)

size
The size of temporary data set that will be required to transfer the load modules

System action

FTP continues.

User response

None.

System programmer response

None.

250-: Unicode to EBCDIC conversion resulted in *number* substitutions

Explanation

The requested data transfer command completed. There were *number* Unicode characters that could not be converted to the EBCDIC code page. Those characters were replaced with the EBCDIC substitution character.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: Waiting for mount for "*dsname*"

Explanation

A CWD command was issued to change the current working directory to *dsname data set* was an existing MVS data set that was catalogued on an unmounted volume. The FTP server needed to mount the volume for the data set in order to determine whether or not the data set was a partitioned data set.

System action

The FTP server waits for the volume to be mounted.

User response

None.

System programmer response

None.

250-: Waiting for recall of "*dsname*"

Explanation

A CWD command was issued to change the current working directory to *dsname*. *dsname* was an existing MVS data set that was migrated. The FTP server needed to recall the data set in order to determine whether or not the data set was a partitioned data set.

System action

The server attempts to recall the data set.

User response

None.

System programmer response

None.

250-: Working Directory for PUT is NULL Device;

250: for GET is "*directory*" partitioned data set.

Explanation

The user entered the CWD *DEV.NULL command to change the current working directory of the server to the NULL directory. When the current working directory is the NULL directory, data transferred to the server from the client (STOR or STOU) will not be stored at the server, but will be received and discarded. The NULL directory is used only for data transferred from the client to the server. Data transferred from the server to the client (RETR) will continue to use the working directory that was in effect prior to the issuance of the CWD *DEV.NULL command. The directory that will be used for the RETR command is the partitioned data set *directory*.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: Working Directory for PUT is NULL Device;

250: for GET is z/OS UNIX directory *directory*

Explanation

The user entered the CWD *DEV.NULL command to change the current working directory of the server to the NULL directory. When the current working directory is the NULL directory, data transferred to the server from the client (STOR or STOU) will not be stored at the server, but will be received and discarded. The NULL directory is used only for data transferred from the client to the server. Data transferred from the server to the client (RETR) will continue to use the working directory that was in effect prior to the issuance of the CWD *DEV.NULL command.

directory is the directory that will be used for the RETR command.

System action

FTP continues.

User response

None.

System programmer response

None.

250-: Working Directory for PUT is NULL Device;

250: for GET is "*directory*" name prefix.

Explanation

The user entered the CWD *DEV.NULL command to change the current working directory of the server to the NULL directory. When the current working directory is the NULL directory, data transferred to the server from the client (STOR or STOU) will not be stored at the server, but will be received and discarded. The NULL directory is used only for data transferred from the client to the server. Data transferred from the server to the client (RETR) will continue to use the working directory that was in effect prior to the issuance of the CWD *DEV.NULL command. The directory that will be used for the RETR command is the MVS high level qualifier *directory*.

System action

FTP continues.

User response

None.

System programmer response

None.

251 reply codes

251: Current working directory is not a PDS

Explanation

The client requested load module transfer processing, and the client current working directory is a PDS, but the server current working directory is a PDSE. Load module transfer processing is only permitted PDS to PDS or PDSE to PDSE. Load module transfer is not supported between different types of load libraries.

System action

The file transfer is aborted. FTP continues, and waits for the next subcommand.

User response

If you want load module transfer processing to be performed, change the server's working directory to a load library that is a PDS.

System programmer response

None.

251: Current working directory is not a PDSE

Explanation

The client requested load module transfer processing, and the client current working directory is a PDSE, but the server current working directory is a PDS. Load module transfer processing is only permitted PDS to PDS or PDSE to PDSE. Load module transfer is not supported between different types of load libraries.

System action

The file transfer is aborted. FTP continues, and waits for the next subcommand.

User response

If you want load module transfer processing to be performed, change the server's working directory to a load library that is a PDSE.

System programmer response

None.

252 reply codes

252: Current working directory is not a load library

Explanation

The client requested load module transfer processing, but the server current working directory is not a load library. A load library is a PDS or a PDSE with RECFM=U.

System action

The file transfer continues using base processing. Any MVS load modules transferred will not be executable on the target system.

User response

If you want load module transfer processing to be performed, change the server's working directory to a load library.

System programmer response

None.

252: No load module transfer processing necessary

Explanation

The client requested load module transfer processing, but the server determined that it is not necessary, because none of the files to be retrieved are actually load modules.

System action

The transfer operation continues using base processing.

User response

None.

System programmer response

None.

253 reply codes

253: Could not build a file list

Explanation

While performing load module transfer, the FTP server was unable to build a list of file names to transfer.

System action

Load module transfer processing ends and base processing continues. Any MVS load modules transferred will not be executable on the target system.

User response

None.

System programmer response

Verify adequate storage available for memory files.

253: No members of the data set match the selection pathnames

Explanation

The client requested load module transfer processing, but there are no files in the server's current working directory that match the selection criteria specified by the client.

System action

FTP continues.

User response

Check file name specified on the GET or MGET subcommand. If applicable, re-issue the GET or MGET command with a correct file name.

System programmer response

None.

254 reply codes

254: Load module transfer requires filetype=SEQ

Explanation

The client requested load module transfer processing, but the server filetype is not SEQ.

System action

Load module transfer processing ends and base processing continues.

User response

If you want load module transfer processing to be performed, send a SITE FILETYPE=SEQ command to the server.

System programmer response

None.

257 reply codes

257: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

257: "'*directory*'" created.

Explanation

The indicated directory was created.

System action

The directory is created. FTP continues.

User response

None.

System programmer response

None.

257: "*directory*" is the z/OS UNIX working directory.

Explanation

The current working directory for storing and retrieving data from the FTP server is a z/OS UNIX directory specified by the *directory* value.

System action

FTP continues.

User response

None.

System programmer response

None.

257: "'*directory*'" is working directory.

Explanation

The current working directory for storing and retrieving data from the FTP server is MVS high level qualifier *directory*.

System action

FTP continues.

User response

None.

System programmer response

None.

257: "'*directory*'" partitioned data set is working directory.

Explanation

If the current working directory is a partitioned data set (PDS), the user PDS name is listed here. For more information about PDSs, see z/OS Communications Server: IP User's Guide and Commands.

System action

FTP continues.

User response

None.

System programmer response

None.

257: MKD failed. Error mounting volume.

Explanation

The MKD command was issued to create the new PDS but the server was unable to mount the volume on which the data set is to be allocated.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Contact the system programmer for the server system.

System programmer response

Determine why the volume could not be mounted and correct the problem.

257: named pipe *pathname* created

Explanation

The FTP server received an XFIF command with the specified path name. The XFIF command is a z/OS FTP proprietary command that directs the FTP server to create a named pipe. The FTP server successfully created a named pipe with the specified path name.

In the message text:

pathname
The name of the named pipe.

Example

```
Command:
quote XFIF /tmp/named.pipe.sample
>>> XFIF /tmp/named.pipe.sample
```

```
257 named pipe /tmp/named.pipe.sample created
Command:
```

System action

Processing continues.

User response

None.

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

257-: Waiting for volume mount for volume *volume*

Explanation

The FTP server must wait for the indicated volume to be mounted before the command can be processed.

System action

The volume is mounted and the command is processed. FTP continues.

User response

None.

System programmer response

None.

257-: Working Directory for PUT is NULL Device;

257: for GET is "*directory*" partitioned data set.

Explanation

The current working directory for data transferred to the server from the client (STOR or STOU) is the NULL directory. Data transferred to the server will be received and discarded rather than stored at the server's host system. MVS Partitioned Data Set *directory* will be used as the current working directory for transferring data from the server to the client (RETR command).

System action

FTP continues.

User response

None.

System programmer response

None.

257-: Working Directory for PUT is NULL Device;

257: for GET is z/OS UNIX directory *directory*.

Explanation

The current working directory for data transferred to the server from the client (STOR or STOU) is the NULL directory. Data transferred to the server will be received and discarded rather than stored at the server's host system. The z/OS UNIX directory specified by the *directory* value will be used as the current working directory for transferring data from the server to the client (RETR command).

System action

FTP continues.

User response

None.

System programmer response

None.

257-: Working Directory for PUT is NULL Device;

257: for GET is "*directory*" name prefix.

Explanation

The current working directory for data transferred to the server from the client (STOR or STOU) is the NULL directory. Data transferred to the server will be received and discarded rather than stored at the server's host system. MVS high level qualifier *directory* will be used as the current working directory for transferring data from the server to the client (RETR command).

System action

FTP continues.

User response

None.

System programmer response

None.

300 reply codes

300: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

300: Restart command accepted, parameter *restart checkpoint*.

Explanation

If a checkpoint for the restart is found by FTP, this reply indicates that the restart is successful. The value for the checkpoint parameter represents the ordinal (number) of the data byte where the restart begins.

System action

FTP continues.

User response

None.

System programmer response

None.

331 reply codes

331: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

331: Send email address as password please.

Explanation

The USER command was entered as anonymous to begin user login processing. The FTP server can be configured to require an email address to validate the anonymous user ID.

System action

FTP continues.

User response

Use the PASS subcommand in FTP to supply your email address to the remote host.

System programmer response

None.

331: Send password please.

Explanation

The USER command was entered to begin user login processing. The FTP server requires a password or password phrase to validate the user ID.

System action

FTP continues.

User response

Use the PASS subcommand in FTP to supply your password or password phrase to the remote host. For more information, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

334 reply codes

334: Using authentication mechanism *mechanism*

Explanation

The client connected to the server and sent an AUTH command requesting an authentication mechanism supported by the server.

mechanism is the authentication mechanism requested by the client

System action

FTP continues.

User response

None.

System programmer response

None.

335 reply codes

335 : ADAT=*base64EncodedData*

Explanation

The client has connected to the server using GSSAPI authentication and sent in an ADAT command. The server must send an ADAT reply containing the authentication data. The server requires another ADAT command from the client.

base64EncodedData is the server's authentication data.

System action

FTP continues.

User response

None.

System programmer response

None.

335 : More data needed

Explanation

The client has connected to the server using GSSAPI authentication and sent in an ADAT command. The server requires another ADAT command from the client.

System action

FTP continues.

User response

None.

System programmer response

None.

350 reply codes

350: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

350: REST command accepted, parameter *byte_transfer_offset*.

Explanation

The server received a REST command from the client. The server accepted the REST command as valid.

byte_transfer_offset is the REST command parameter.

System action

FTP continues. The next file transfer will start at *byte_stream_offset* within the stream of bytes that would be transmitted if the whole file were transferred.

User response

If the client is trying to resume an interrupted file transfer, no further action is needed. If the client does not want to resume an interrupted file transfer, issue quote REST 0 from the FTP client to nullify the REST command.

System programmer response

None.

350: RNFR accepted. Please supply new name for RNTO.

Explanation

The RNFR command, which specifies the data set to be renamed, was accepted. The FTP server is prompting the user to supply the new name for the data set.

System action

FTP continues.

User response

Use the RNTO command to specify the new name for the data set to be renamed. See the z/OS Communications Server: IP User's Guide and Commands, in the information about transferring data using

the file transfer protocol for information about the RNFR and RNTO subcommands, or type HELP RNTO at the command line.

System programmer response

None.

400 reply codes

400: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

421 reply codes

421: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

421: connection terminated - setuid failure during REIN command processing. *error*

Explanation

The client entered the REIN command to reinitialize an FTP session back to the state of a new connection that has not logged in as user ID. In order to reset the user ID to a new user ID or to a state of no user ID, the server must change the user ID associated with the server to a superuser user ID. The server was unable to return to the superuser environment.

error is the LE run-time library error message for the failure. See the z/OS Language Environment Runtime Messages for a complete description of *error*.

System action

The FTP session ends.

User response

Try the connection and the failing command again. If the problem persists, contact the system programmer.

System programmer response

Determine the cause of the error using the information contained in the message and correct the problem.

421: Open rejected due to insufficient resources.

Explanation

The FTP server attempted to create a new address space for the client session, but was unable to do so.

System action

FTP continues. The client connection ends.

User response

If the problem persists, contact the system programmer.

System programmer response

If necessary, re-create the problem with tracing. The trace messages will show the exact error received by the server when it attempted to fork the new address space. Correct the error indicated by the traces.

421: User Exit rejects open for connection.

Explanation

The FTP server is running with the security user exit FTCHKIP. The user exit does not allow the IP address to access the FTP server.

System action

FTP continues. The client connection is rejected.

User response

Contact the owner of the FTP server to have the IP address authorized in the FTCHKIP user exit.

System programmer response

If necessary, update the FTCHKIP user exit to allow the IP address to access the server.

425 reply codes

425: Can't open data connection.

Explanation

The server cannot open the data connection to transfer the data set.

System action

The data set is not transferred. FTP continues.

User response

None.

System programmer response

If necessary, re-create the problem with FTP server trace active. The data connection error will create a trace record with a socket function return code. Determine the cause of the socket error and correct the problem.

425: Can't open passive connection.

Explanation

The FTP server received a PASV or EPSV command requesting that the server open a passive data connection (server does the “listen” rather than the “connect”). The server was unable to open the passive connection.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

If necessary, re-create the problem with FTP server trace active. The open data connection error will create a trace record with a socket function return code. Determine the cause of the socket error and correct the problem.

425: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

425-: Server requires protected data connection.

Explanation

The FTP server processed a command that requires a data connection. The session is protected by a security mechanism and the protection level for the data connection is Clear. The minimum data connection protection required by the server is Safe or Private.

System action

FTP continues.

User response

If you are using the z/OS FTP client, issue the PROTect SAFE or PROTect PRIVATE subcommand to set the protection level for data transfers on the data connections.

System programmer response

None.

425: Unable to open data connection.

Explanation

The server cannot open the data connection to transfer the data.

System action

The data is not transferred. FTP continues.

User response

None.

System programmer response

If necessary, re-create the problem with FTP server trace active. The data connection error will create a trace record with a socket function return code. Determine the cause of the socket error and correct the problem.

426 reply codes

426: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

426: Connection closed; transfer aborted.

Explanation

The FTP server received an Out Of Band ABOR command from the FTP client requesting that the data transfer in progress end. The FTP server aborted the data transfer.

System action

The data transfer in progress is aborted. FTP continues.

User response

None.

System programmer response

None.

426: Data connection aborted

Explanation

The FTP server closed the data connection because of an error reported in a previous reply.

System action

FTP continues.

User response

None.

System programmer response

None.

426-: Data set *dsname* is allocated to another job and is unavailable for *cmd* command.

Explanation

The *cmd* command was issued but the server was unable to allocate the data set because it is already allocated to another job.

System action

None.

User response

Try again later.

System programmer response

None.

450 reply codes

450: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

450: Data set *dsname* is allocated to another job and is unavailable for *cmd* command.

Explanation

The *cmd* command was issued but the server was unable to allocate the data set because it is already allocated to another job.

System action

None.

User response

Try again later.

System programmer response

None.

450: JESGET failed, could not allocate send buffer

Explanation

While attempting to send a file, a buffer was not available.

System action

FTP continues.

User response

Reissue the command later.

System programmer response

None

450-: Record too long

Explanation

During the transmission of a file, an incomplete record was encountered.

System action

FTP continues.

User response

Reissue the command.

System programmer response

None

450: timer expired waiting for read process to open *pathname*

Explanation

The FTP server received a STOR (store) or APPE (append) command while UNIXFILETYPE=FIFO was configured. When UNIXFILETYPE=FIFO is configured, the target of a STOR or APPE command is a named pipe instead of a regular z/OS UNIX file. The FTP server cannot write to a named pipe until another process opens the named pipe for reading. The FTP server waited for the number of seconds specified by the FIFOOPENTIME configuration option for another process to open the specified path name. The FIFOOPENTIME time limit expired before a process could open the specified path name for reading.

See the UNIXFILETYPE (FTP client and server) statement and the FIFOOPENTIME (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference for more information about these configuration options.

In the message text:

pathname
The path name of the named pipe.

Example

```
 put /etc/hosts /tmp/etc.hosts.fifo
>>> PORT 9,2,1,3,4,35
200 Port request OK.
>>> STOR /tmp/etc.hosts.fifo
125-Waiting for read process to open /tmp/etc.hosts.fifo
125 Transfer request aborted
450 timer expired waiting for read process to open /tmp/etc.hosts.fifo
Command:
```

System action

FTP fails the file transfer command.

User response

Perform the following steps:

1. Increase the FIFOOPENTIME configured value before attempting the file transfer again.
   - From the z/OS FTP client:
     a. Issue the STAT (FIFOOPENTIME subcommand to determine the FIFOOPENTIME configured value.
     b. Issue the SIte subcommand with the FIFOOPENTIME parameter to specify a larger value.
   - From any FTP client:
     a. Use the QUOTE subcommand to send an XSTA (FIFOOPENTIME command to the FTP server to determine the FIFOOPENTIME configured value.
     b. Use the QUOTE subcommand to send a SITE command with the FIFOOPENTIME parameter to the FTP server to specify a larger value.
   - See the information about the SIte subcommand and the STAtus subcommand in z/OS Communications Server: IP User's Guide and Commands for information about the FIFOOPENTIME configuration option.
2. Reissue the FTP subcommand that caused the FTP client to send the STOR or APPE command to the FTP server.

If these actions do not resolve the problem, notify the system programmer.

System programmer response

Start a process at the FTP server host to read from the path name specified by the *pathname* value, and tell the user to attempt the file transfer again.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

450: timer expired waiting for write process to open *pathname*

Explanation

The FTP server received a RETR command while UNIXFILETYPE=FIFO was configured. When UNIXFILETYPE=FIFO is configured, the target of a RETR command is a named pipe instead of a regular z/OS UNIX file. The FTP server cannot read from a named pipe until another process opens the named pipe for writing. The FTP server waited for the number of seconds specified by the FIFOOPENTIME configuration option for another process to open the specified path name. The FIFOOPENTIME time limit expired before a process could open the specified path name for writing.

See the UNIXFILETYPE (FTP client and server) statement and the FIFOOPENTIME (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference for more information about these configuration options.

In the message text:

pathname
The path name of the named pipe.

Example

```
Command:
get new.fifo
>>> PORT 9,42,105,36,4,59
200 Port request OK.
>>> RETR new.fifo
125-Waiting for write process to open /tmp/trash/new.fifo
125 Transfer request aborted
450 timer expired waiting for write process to open /tmp/trash/new.fifo
Command:
```

System action

FTP fails the file transfer command.

User response

Perform the following steps:

1. Increase the FIFOOPENTIME configured value before attempting the file transfer again.
   - From the z/OS FTP client:
     a. Issue the STAT (FIFOOPENTIME subcommand to determine the FIFOOPENTIME configured value.
     b. Issue the SIte subcommand with the FIFOOPENTIME parameter to specify a larger value.
   - From any FTP client:

a. Use the QUOTE subcommand to send an XSTA (FIFOOPENTIME command to the FTP server to determine the FIFOOPENTIME configured value.
b. Use the QUOTE subcommand to send a SITE command with the FIFOOPENTIME parameter to the FTP server to specify a larger value.

- See the information about the SIte subcommand and the STAtus subcommand in z/OS Communications Server: IP User's Guide and Commands for information about the FIFOOPENTIME configuration option.

2. Reissue the FTP subcommand that caused the FTP client to send the RETR command to the FTP server.

If these actions do not resolve the problem, notify the system programmer.

System programmer response

Start a process at the FTP server host to write to the path name, and tell the user to attempt the file transfer again.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

450: timer expired while reading from named pipe

Explanation

The server received a RETR command that specified a named pipe in the z/OS UNIX file system. The server was able to open the named pipe, and was reading data from the named pipe. For the number of seconds specified by the FIFOIOTIME configuration option, the server could not read data from the named pipe. The FIFOIOTIME timer expired, which cancelled the read of the named pipe.

A possible cause of this error is that the process that writes data to the named pipe on the server host stopped writing data without closing the named pipe.

Any data sent from the server to client before the timer expired was permanently removed from the named pipe.

For more information about named pipes and the FIFOIOTIME configuration option, see the following topics:

- The FIFOIOTIME (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference.
- The SIte subcommand in z/OS Communications Server: IP User's Guide and Commands .
- The information about using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User's Guide and Commands.

Example

```
Command:
stat (fifoiotime
>>> XSTA (fifoiotime
211-Timer FIFOIOTIME is set to 31
211 *** end of status ***
Command:
get /tmp/fifo.sample (rep
>>> PORT 9,42,105,36,4,5
200 Port request OK.
>>> RETR /tmp/fifo.sample
```

```
125 Sending data set /tmp/fifo.sample
450 timer expired while reading from named pipe
Confidence=Low for GET of /SYSTEM/tmp/CAPI/fifo.sample
Command:
```

System action

The server cancels the current file transfer, and waits for the next command.

User response

Report the error to the system programmer.

System programmer response

Perform the following steps:

1. Increase the FIFOIOTIME configured value.
   a. Issue the STAT (FIFOIOTIME command to query the current FIFOIOTIME value.
   b. Use the SITE command with the FIFOIOTIME parameter to increase the FIFOIOTIME value.

   If you anticipate long idle periods, consider using keepalive packets for the control and data connections. For more information about keepalive packets, see the following topics:
   - The FTPKEEPALIVE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference.
   - The DATAKEEPALIVE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference.
   - The information about configuring PROFILE.TCPIP for FTP in z/OS Communications Server: IP Configuration Guide.
2. Determine why the process that writes to the named pipe stopped writing data, but did not close the named pipe.
3. Reissue the subcommand that failed when the FIFOIOTIME timer expired. Any data sent from the server to the client before the timer expired has been removed from the named pipe. You must take this into consideration before repeating the file transfer.

Problem determination

See the system programmer.

Source

z/OS Communications Server TCP/IP: FTP

450: Cannot create unique data set name for store unique of dsname

Explanation

A unique name cannot be created to store a data set by using the store unique command. The server has tried to create the data set for the maximum number of 10 times, and each time it experiences a name collision with another server thread or batch job.

System action

The command is rejected. FTP continues.

User response

Change the file name for the store-unique command or try again later.

System programmer response

None.

451 reply codes

451-: Checkpoint marker not supported

Explanation

A store request failed for a variable spanned data set because a block header contains a checkpoint/restart marker. Checkpointing is not supported from transfers to a variable spanned data set when the logical record length is larger than the blocksize.

System action

FTP continues.

User response

Ensure that the client program is not sending checkpoint markers. For the MVS client, issue LOCSITE CHKPTINT=0 and try the transfer again.

System programmer response

None.

451: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

451-: Compression reduced bytes transferred by *percentage* percent

Explanation

Data is being transferred while in mode c (compressed). The compression algorithm has reduced the number of bytes of data that are transferred for the request by the percentage shown in by *percentage*.

System action

FTP continues.

User response

None.

System programmer response

None.

451-: Data set is full (19).

Explanation

A store request failed because the destination data set is full. The C run-time errno code of 19 indicates that an unrecoverable error has permanently marked the data set in error.

System action

FTP continues.

User response

Request a larger space allocation for the destination data set and try the transfer again.

System programmer response

None.

451-: Data set is full *rc*.

Explanation

A store request failed because the destination data set is full. The C run-time errno code of 33 says that an attempt was made to extend a non-extendable file. The C run-time errno code of 65 says that a write system error occurred.

System action

FTP continues.

User response

Request a larger space allocation for the destination data set and try the transfer again.

System programmer response

None.

451-: Data set is out of space.

Explanation

A data transfer failed because there is not enough space in the data set.

System action

FTP continues.

User response

This reply is preceded by a reply with the specific system completion code and reason code. Take actions appropriate for the failure.

System programmer response

None.

451: data transfer aborted - command terminated due to CPU time limit exceeded.

Explanation

The FTP server was in the process of transferring data when the process was stopped either by an OMVS kill -s SIGXCPU command or because the CPU time limit (MAXCPUTIME in BPXPRMnn) was exceeded.

System action

Data transfer and the FTP server process end.

User response

Contact the system programmer.

System programmer response

If the process was stopped due to CPU time limit exceeded, check the MAXCPUTIME in the BPXPRMnn member.

451: data transfer aborted - command terminated due to server shutdown in progress

Explanation

The FTP server was in the process of transferring data when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

Data transfer and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

451: Dele failed due to internal error

Explanation

A required data area was not available for the requested JES function to complete.

System action

FTP continues.

User response

Reissue the command later.

System programmer response

None.

451: Dele failed, too many entries

Explanation

A request was made to JES to delete multiple job IDs. To many jobs exist for JES to process this request.

System action

FTP continues.

User response

Reissue the command. If the problem persists, request assistance from your system support personnel.

System programmer response

None.

451-: Device is out of space.

Explanation

A file transfer to the FTP server z/OS UNIX file system failed. The C runtime library reported the error as 'device out of space', indicating that the target directory is out of space.

System action

The file transfer fails. FTP continues processing.

User response

Report the error to the system programmer.

System programmer response

Create more space in the target directory by deleting files, or instruct the user to store the file in a different location with adequate space.

451: Error (*error*) closing the data set.

Explanation

The data set or file did not close successfully.

error is the fclose() return code when the file is a z/OS UNIX file. *error* is not meaningful otherwise.

System action

FTP continues.

User response

None.

System programmer response

None.

451: Error (*error*) closing the data set. File could not be deleted.

Explanation

The MVS data set did not close successfully. The FTP server tried to delete the data set because the current CONDDISP is set to delete the data set when a close failure occurs.

error is not meaningful.

System action

FTP continues processing.

User response

Change the CONDDISP setting with a SIte subcommand if you do not want data sets to be deleted when the close fails. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

None.

451: Error (*error*) closing the data set. File is catalogued.

Explanation

The MVS data set did not close successfully. The data set was catalogued.

error is not meaningful.

System action

FTP continues processing.

User response

Change the CONDDISP setting with a SIte subcommand if you do not want data sets to be catalogued when file transfers fail. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

None.

451: Error (*error*) closing the data set. File is deleted.

Explanation

The MVS data set did not close successfully. The data set was deleted.

error is not meaningful.

System action

FTP continues processing.

User response

Change the CONDDISP setting with a SIte subcommand if you do not want data sets to be deleted when the close fails. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

None.

451: Error *(rc)* closing the data set *dsname*

Explanation

The close of the data set was unsuccessful.

System action

FTP continues.

User response

None.

System programmer response

Reissue the command.

451-: File transfer failed. File contains records that are longer than the LRECL of the new file.

Explanation

Options NOTRUNcate and NOWRAPrecord are set. The file being transferred contains records that are longer than the LRECL of the new file.

System action

The transfer is ended. FTP continues.

User response

Increase the value of LRECL for the new file or change the Locsite options.

System programmer response

None.

451: File transfer failed. Multi-byte data conversion error occurred

Explanation

The data cannot be translated using the iconv() code conversion library function. One or more codepoints in the data cannot be converted.

System action

FTP continues.

User response

Issue the following command to gather information about the conversion failure:

```
SITE DEBUG=FSC DUMP=42
```

Reissue the file transfer subcommand that failed and contact the system programmer to request the server trace of the failed conversion attempt. The DEBUG parameter generates a display of the reason the conversion failed. For some types of conversion errors, the DUMP parameter generates a display of the actual data that could not be converted.

If you are not allowed to issue the SITE command to change the server trace options, ask the system programmer to set the debug and dump options with a MODIFY command to the FTP server, close the session to the server, enter FTP again and reissue the failing subcommand.

System programmer response

None.

451: File Transfer might not be complete. Last record received without EOL sequence.

Explanation

FTP received the last record of a file but there were no end of line (EOL) characters. The file transfer might not be complete. FTP appends the EOL characters and processes the rest of the data as a complete record.

System action

If the FTP.DATA CONDDISP option is set to CONDDISP=CATALOG, the file is saved. If the FTP.DATA CONDDISP option is set to CONDDISP=DELETE the file is deleted.

User response

If the file was saved, verify that the file transferred is correct. If the file was deleted, set CONDDISP to CATALOG and transfer the file again.

System programmer response

None.

451: Index *index* is greater than number of spool files for *jobid*

Explanation

A specific spool file was requested to be retrieved from JES using the FTP GET command. JES output files are numbered sequentially from one. The specified number is greater than the number of spool files for the job.

System action

FTP continues.

User response

Reissue the FTP GET command with the correct job ID and index.

System programmer response

None.

451: Internal storage allocation error, JesPutGet aborted

Explanation

While attempting to retrieve an output file for a JOB, an insufficient storage condition existed.

System action

FTP continues.

User response

Reissue the command later.

System programmer response

None.

451: Internal storage allocation error, try again later

Explanation

While attempting to retrieve an output file for a JOB, an insufficient storage condition existed.

System action

FTP continues.

User response

Reissue the command later.

System programmer response

None.

451: JESGET aborted: internal error processing JES request

Explanation

FTP encountered an internal error with the JES interface. Partial data might be sent.

System action

FTP continues.

User response

Try the request again. If the problem persists, contact the system programmer for FTP.

System programmer response

If the problem persists, get a trace of the FTP operation that includes the FTP JES trace and contact the IBM Software Support Center.

451: JESPUTGET aborted: internal error processing JES request

Explanation

FTP encountered an internal error with the JES interface. Partial data might be sent.

System action

FTP continues.

User response

Try the request again. If the problem persists, contact the system programmer for FTP.

System programmer response

If the problem persists, get a trace of the FTP operation that includes the FTP JES trace and contact the IBM Software Support Center.

451: List failed due to internal error

Explanation

A required data area was not available at the time the command was issued.

System action

FTP continues.

User response

Reissue the command later.

System programmer response

None.

451: List failed, too many entries

Explanation

The request resulted in more data than the data area could contain.

System action

FTP continues.

User response

Reissue the command later. If the problem persists, request assistance from system support personnel.

System programmer response

None.

451-: LRECL *lrecl* is incompatible with RECFM *recfm*

Explanation

The LRECL value is incompatible with the RECFM. This value might have come from FTP.DATA, as the result of a SITE command, or from MVS as a default.

lrecl is the length of the record.

recfm is the record format.

System action

The file transfer ends.

User response

Enter a correct value using SITE LRECL=*value*. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Update the server FTP.DATA file. See the z/OS Communications Server: IP Configuration Reference for information about coding statements in the FTP.DATA file.

451: Nlst failed due to internal error

Explanation

A required data area was not available at the time the command was issued.

System action

FTP continues.

User response

Reissue the command later.

System programmer response

None.

451: Nlst failed, too many entries

Explanation

The request resulted in more data than the data area could contain.

System action

FTP continues.

User response

Reissue the command later. If the problem persists, request assistance from system support personnel.

System programmer response

None.

451-: Possible cause is the destination PDS or its directory is too small.

Explanation

An ABENDB14 has occurred. This might have been preceded by an ABENDD37. This would imply that the destination data set is too small. This reply is to warn the client of that possibility.

System action

The FTP session ends.

User response

Take action as is appropriate for the B14 and D37 abend codes. Verify with operations that a D37 did occur or try increasing the size of the PDS of the directory.

System programmer response

Verify that this is a recursive abend and take action as suggested by the abend that occurred.

451-: Record is too long to process

Explanation

A file from an ASCII client is FTP PUT to the server. SITE NOWRAP is set, and data type is ASCII. The file has an extremely long record and cannot be transferred.

System action

The data transfer is terminated and the data session is closed.

User response

Set Wraprecord on or correct the source file. Insert Carriage Returns as needed to break up the line or delete the invalid line.

System programmer response

None.

451-: Record received was too short (4).

Explanation

A store request failed because one of the records that is transferred is too short for the destination data set. This error occurs when the destination data set is a fixed record format, the transfer mode is b (blocked) or c (compressed), and a short record is transferred. The C run-time errno code of 4 says that a specified record length is not large enough.

System action

FTP continues.

User response

Ensure that each fixed format record has the correct length or choose a non-fixed record format (for example, a variable).

System programmer response

451: Renaming attempt failed.

Explanation

A RNTO command was issued to rename a member of a partitioned data set. The rename was unsuccessful because a system resource was not available.

System action

The data set is not renamed. FTP continues.

User response

None.

System programmer response

If possible, re-create the problem with FTP server trace active and contact the IBM Support Center with the results.

451-: System completion code and reason: *cc-rc*

Explanation

The transfer of data ended because of a file I/O error. The system completion code *cc* and reason code *rc* are displayed.

System action

FTP continues.

User response

See the *System Codes* and the *System Messages* publications for suggested actions for the specified failure code.

System programmer response

None.

451: Transfer aborted.

Explanation

The transfer of data ended because of an error in the block header of the data.

System action

Processing continues.

User response

None.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to file error.

Explanation

The transfer of data ended because of an error while writing to the data set.

System action

Processing continues.

User response

None.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to file error. File could not be deleted.

Explanation

The transfer of data ended because of an error while writing to the data set. The FTP server tried to delete the data set because the current CONDDISP is set to delete the data set when write errors occur.

System action

Processing continues.

User response

Change the CONDDISP setting with a SITE command if you do not want data sets deleted when file write errors occur. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to file error. File is catalogued.

Explanation

The transfer of data ended because of an error while writing to the data set. The data set was catalogued.

System action

Processing continues.

User response

Change the CONDDISP setting with a SITE command if you do not want data sets catalogued when file write errors occur. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to file error. File is deleted.

Explanation

The transfer of data ended because of an error while writing to the data set or file.

System action

Processing continues.

User response

Change the CONDDISP setting with a SITE command if you do not want data sets deleted when file write errors occur. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to receive error.

Explanation

The transfer of data ended because of an error while receiving data from the data connection.

System action

Processing continues.

User response

None.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to receive error. File could not be deleted.

Explanation

The transfer of data ended because of an error while receiving data from the data connection. The FTP server tried to delete the data set because the current CONDDISP is set to delete the data set when close failures occur.

System action

Processing continues.

User response

Change the CONDDISP setting with a SIte subcommand if you do not want data sets to be deleted when the close fails. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to receive error. File is catalogued.

Explanation

The transfer of data ended because of an error while receiving data from the data connection. The partially transferred file was catalogued.

System action

Processing continues.

User response

Change the CONDDISP setting with a SITE command if you do not want data sets catalogued when receive errors occur. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted due to receive error. File is deleted.

Explanation

The transfer of data ended because of an error while receiving data from the data connection. The partially transferred file or data set is deleted.

System action

Processing continues.

User response

Change the CONDDISP setting with a SIte subcommand if you do not want data sets to be deleted when the close fails. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted. File could not be deleted.

Explanation

The transfer of data ended because of an error in the block header of the data. The FTP server tried to delete the data set because the current CONDDISP is set to delete the data set when file transfer errors occur.

System action

Processing continues.

User response

Change the CONDDISP setting with a SITE command if you do not want data sets deleted when file write errors occur. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted. File is catalogued.

Explanation

The transfer of data ended because of an error in the block header of the data.

System action

Processing continues.

User response

Change the CONDDISP setting with a SITE command if you do not want data sets catalogued when file transfer errors occur. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted. File is deleted.

Explanation

The transfer of data ended because of an error in the block header of the data. The data set was deleted.

System action

Processing continues.

User response

Change the CONDDISP setting with a SITE command if you do not want data sets deleted when file write errors occur. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System programmer response

Get a trace of the store operation and contact the IBM Software Support Center.

451: Transfer aborted: file error.

Explanation

The transfer of data ended because of an error reading the data set.

System action

FTP continues.

User response

None.

System programmer response

Get a trace of the retrieve operation and contact the IBM Software Support Center.

451: Transfer aborted: internal error while processing SQL request

Explanation

FTP encountered an internal error while processing a SQL request. No data is sent.

System action

FTP continues.

User response

Try again. If the problem persists, contact the system programmer for FTP.

System programmer response

If the problem occurs repeatedly, get a trace of the FTP operation and contact the IBM Support Center.

451: Transfer aborted: send error.

Explanation

The server was attempting to send data to the client over the data connection, but an error occurred executing the send() socket function for the data connection. The data transfer is ended.

System action

Control is returned to the client connection for further command processing.

User response

The command can be tried again. If the problem persists, contact the system programmer

System programmer response

If necessary, re-create the problem with FTP server traces active. The send() error will create a trace record with the send() return code. Determine the cause of the send error and correct the problem.

451: Transfer aborted: SQL FETCH error *(code)*

Explanation

A SQL query was submitted through FTP, but Db2 encountered an error retrieving the data. Data retrieval for this query is discontinued. Data in the output file might be incomplete. *code* indicates the reason for the failure.

System action

FTP continues.

User response

Resubmit the query. If the problem persists, contact the system programmer for FTP.

System programmer response

See "SQL Return Codes" in the *Db2 Messages and Codes* for an explanation of *code* and correct the problem.

451: Transfer completed

Explanation

A job was successfully submitted,

System action

FTP continues.

User response

None.

System programmer response

None.

451-: Unable to get Jobid

Explanation

A job was submitted to JES. No Jobid was returned after the completion of the submit.

System action

FTP continues.

User response

Check the JCL file for an error in the JOBCARD.

System programmer response

None.

451: Unrecoverable error from JES SSI request RC=*rc*

Explanation

An unexpected error occurred using the Subsystem Interface (SSI).

rc is the decimal return code from SSI.

System action

FTP continues.

User response

See your system programmer.

System programmer response

See the z/OS MVS Using the Subsystem Interface for a description of the return code. If you are unable to correct the problem, see the z/OS Communications Server: IP Diagnosis Guide for information about diagnosing errors and reporting them to the IBM Software Support Center.

452 reply codes

452: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

452: insufficient storage to process SITE command

Explanation

The SITE command was entered, but there was not enough storage available for the server to parse the SITE command.

System action

FTP continues.

User response

Try the command at a later time when more storage might be available.

System programmer response

None.

452: Transfer aborted: insufficient storage to process SQL request

Explanation

A SQL query was being attempted through FTP, but there is not enough system storage available for FTP to compete the request.

System action

No data is sent. FTP continues.

User response

Try again. If the problem persists, contact the system programmer for the FTP server.

System programmer response

Determine why FTP is unable to acquire dynamic storage and correct the problem.

500 reply codes

500: Command failed - command too long

Explanation

The FTP server attempted to receive a command from the client connection, but the command received was larger than the FTP server command buffer. The maximum allowed command length is 1099 bytes, including control characters.

System action

The command is rejected. Control returns to the client connection for further command processing.

User response

If possible, break the command into multiple, smaller, commands (for example, a SITE command with multiple parameters can be broken into several SITE commands with fewer parameters). If it is not possible to break the command into smaller pieces, contact the IBM $ Software Support Center with requirements for a larger command buffer.

System programmer response

None.

500: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

500: Invalid restart parameter.

Explanation

You attempted to restart a checkpointed data transfer command and the restart marker that was received at the server is incorrect.

System action

The data transfer command is not restarted. FTP continues.

User response

Make sure that the *hlq*.FTP.CHECKPOINT data set is valid. The data set name might be *hlq*.FTP.CHECKPOINT or, if your path points to a PDS, the name will be *hlq*.pds_name(CHKPOINT). This data set was created by the client during a checkpointed command and must not be altered after the checkpointed command is unsuccessful and before the restart is entered. Failure to observe this procedure will affect the restart.

System programmer response

None.

500: unknown command *command*

Explanation

The client connection entered the command *command*, which the FTP server did not recognize as a valid FTP command.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

Issue a valid FTP command.

System programmer response

None.

500: User Exit denies user from using Command '*command*'.

Explanation

The client logged in to the server as anonymous attempted to issue the FTP command *command*. The FTP server was running with the user-written exit routine FTCHKCMD, and the FTCHKCMD user exit prevented the user from issuing command *command*.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

See the preceding 500-UX- reply (if generated by the user exit) for an explanation of the rejection. Contact the system programmer for the server system for more information.

System programmer response

If necessary, change the user exit FTCHKCMD to allow the user to issue the command. The client must end the FTP session and then reconnect to the server in order to pick up changes to the user exit routines.

500: User Exit denies Userid '*user_ID*' from using Command '*command*'.

Explanation

The client logged in to the server as user ID *user_ID* and attempted to issue the FTP command *command*. The FTP server was running with the user-written exit routine FTCHKCMD, and the FTCHKCMD user exit prevented the user ID *user_ID* from issuing command *command*.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

See the preceding 500-UX- reply (if generated by the user exit) for an explanation of the rejection. Contact the system programmer for the server system for more information.

System programmer response

If necessary, change the user exit FTCHKCMD to allow the user to issue the command. The client must end the FTP session and then reconnect to the server in order to pick up changes to the user exit routines.

500-: UX-*explanation*

Explanation

This reply precedes the notification that the user exit has denied the user access to this command.

explanation is the exit routine's explanation of why the user was denied access to the command.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer for the server system for more information if needed.

System programmer response

If necessary, change the user exit FTCHKCMD to allow the user to issue the command. The client must end the FTP session and then reconnect to the server to pick up changes to the user exit routines.

501 reply codes

501: * is not last char

Explanation

The LIST or NLST command was entered with the * global file-name character in the path name, but the * was not the last character in the qualifier. For MVS FTP, the * global file-name character can only appear at the end of any qualifier in the data set name.

System action

The LIST or NLST command is rejected.

User response

Issue the command again with the correct syntax.

System programmer response

None.

501: ** must be preceded and followed by a period or blank

Explanation

The LIST (DIR) or NLST (LS) command was entered with the ** global file name character in the path name, but the ** was either not preceded by or not followed by a period (.) or blank. The ** character is used to replace zero or more complete qualifiers in the name.

System action

FTP continues.

User response

See the z/OS Communications Server: IP User's Guide and Commands for the rules for using special characters in LIST and NLST commands.

System programmer response

None.

501: A qualifier in "*pathname*" begins with an invalid character

Explanation

The path name in the subcommand entered specified an MVS data set, but one of the qualifiers in the data set name began with an invalid character. Qualifiers in an MVS data set name can only begin with a letter, a dollar sign ($), an at sign (@), or a number sign (#).

System action

The subcommand is rejected. Control returns to the client for further command processing.

User response

Reissue the subcommand with the corrected path name.

System programmer response

None.

501: A qualifier in "*pathname*" is more than 8 characters

Explanation

The path name in the subcommand entered specified an MVS data set, but one of the qualifiers in the data set name was longer than 8 characters. Qualifiers in an MVS data set name cannot exceed 8 characters.

System action

The subcommand is rejected. Control returns to the client for further command processing.

User response

Reissue the subcommand with the corrected path name.

System programmer response

None.

501: A qualifier in "*pathname*" contains an invalid character

Explanation

The path name in the subcommand entered specified an MVS data set, but one of the qualifiers in the data set name contained an invalid character. Qualifiers in an MVS data set name can only contain letters, numbers, a dollar sign ($), an at sign (@), a number sign (#), a hyphen (-), or a ‘x'C0''.

System action

The subcommand is rejected. Control returns to the client for further command processing.

User response

Reissue the subcommand with the corrected path name.

System programmer response

None.

501 : Base 64 decode failed for ADAT data: *error*

Explanation

The server received an ADAT command containing authentication data but was unable to decode the authentication data.

error can be one of the following values:

1

Bad character in encoding: An invalid character was received from the server as part of a base 64 encoded string. The valid characters in a base 64 encoded string are the letters A–Z, the letters a–z, the numbers 0–9, the plus sign (+), and the forward slash (/).

2

Encoding not properly padded: An invalid base 64 encoded string was received from the server. The string was not padded with equal signs to extend the length of the string to a multiple of four characters.

3

Decoded number of bits not a multiple of 8: An invalid base 64 encoded string was received from the server. The string was unable to be decoded because it did not decode into a multiple of eight bits.

System action

Authentication negotiation fails. FTP continues.

User response

Contact the system programmer of the client to determine why the authentication data was not properly base 64 encoded.

System programmer response

None.

501 : Base 64 decode failed for *command* command: *error*

Explanation

The server received a base 64 encoded command and was unable to decode the command.

command is the type of protected command. Valid values are ENC for protection level private commands and MIC for protection level safe commands.

error can be one of the following values:

1

Bad character in encoding: An invalid character was received from the server as part of a base 64 encoded string. The valid characters in a base 64 encoded string are the letters A–Z, the letters a–z, the numbers 0–9, the plus sign (+), and the forward slash (/).

2

Encoding not properly padded: An invalid base 64 encoded string was received from the server. The string was not padded with equal signs to extend the length of the string to a multiple of four characters.

3

Decoded number of bits not a multiple of 8: An invalid base 64 encoded string was received from the server. The string was unable to be decoded because it did not decode into a multiple of eight bits.

System action

The command fails. FTP continues.

User response

Contact the system programmer of the client to determine why the authentication data was not properly base 64 encoded.

System programmer response

None.

501: command aborted - error in local processing

Explanation

An internal programming error occurred that caused the parser to end up within the routines that process the valid FTP commands while processing an incorrect command.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer of the FTP server system.

System programmer response

Contact the IBM Software Support Center. The FTP server output should provide additional information regarding the failure.

501: command aborted -- FTP server not configured for *commandname*

Explanation

The client issued a *command name* command to the FTP server. The FTP server implements the *command name* command, but is configured to reject it.

System action

The command is rejected. Control is returned to the client connection for further command processing.

User response

Report the error to the FTP server installation system programmer.

System programmer response

If you want your FTP server to support *command name*, add statements to FTP.DATA to enable this support. See the z/OS Communications Server: IP Configuration Reference for information on enabling *command name* support for your FTP server.

501: command *command* fails: "" is not a valid directory name

Explanation

The FTP server received a command containing a pair of quotation marks (""), indicating an empty quoted string as a directory argument, but "" is not a valid directory name.

command is the command that specified the "" directory name.

System action

The command is rejected. Control returns to the client for further command processing.

User response

Reissue the command with a valid directory name.

System programmer response

None.

501: *command* command syntax error : too many parameters

Explanation

The client issued the FTP command *command*, but the command contained more parameters than allowed for that command.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

Reissue the command with the correct number of parameters.

System programmer response

None.

501: command OPTS aborted -- no options supported for *command*

Explanation

The server received an OPTS command. The server does not support any options for *command*.

command is the argument of the OPTS command.

See RFC 2389 for more information about the OPTS command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

The OPTS command is ignored. Processing continues.

User response

None.

System programmer response

None.

501: *command* supported only in Stream mode

Explanation

The LIST or NLST command was entered, but the FTP session was in a mode other than stream mode. The LIST and NLST command are supported only in stream mode.

System action

The LIST or NLST command is rejected.

User response

Issue the MODE S command to change the mode to stream mode, then reissue the LIST or NLST command.

System programmer response

None.

501: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

501: CWD ../ only valid for z/OS UNIX directories

Explanation

The CWD command was entered with a path name of ../ to back up one directory level, but the current working directory was either an MVS partitioned data set, or an MVS high level qualifier. The ../ notation is valid only when the current working directory is a z/OS UNIX directory.

System action

The CWD command is rejected. Control returns to the client for further command processing.

User response

Reissue the CWD command with the corrected path name.

System programmer response

None.

501: Data set name too long. Use MVS naming conventions.

Explanation

The LIST or NLST command was entered with a data set name that was longer than the MVS maximum of 44 characters.

System action

The LIST or NLST command is rejected.

User response

Reissue the LIST or NLST command with the correct data set name.

System programmer response

None.

501: Data set name too long. Use MVS or z/OS UNIX data set naming conventions.

Explanation

The LIST or NLST command was entered with a data set name that was longer than the MVS maximum of 44 characters or the z/OS UNIX maximum of 1023 characters.

System action

The LIST or NLST command is rejected.

User response

Reissue the LIST or NLST command with the correct data set or z/OS UNIX file name.

System programmer response

None.

501: '*data_set(member)*' requests members but *data_set* is not a partitioned data set.

Explanation

The LIST or NLST command was entered using the MVS syntax *data_set(member)*, which indicates that members of the PDS *data_set* are to be listed; however, *data_set* is not a partitioned data set.

System action

The LIST or NLST command is rejected.

User response

Verify that the correct data set name was entered. Reissue the LIST or NLST command with the correct data set name.

System programmer response

None.

501: Directory is already NULL

Explanation

The CDUP, or CD .. command was issued to back up the directory name one level, but the directory name was already back to the NULL directory ("").

System action

The CDUP command is rejected.

User response

None.

System programmer response

None.

501: Error - existing kanji type invalid

Explanation

The FTP server received an invalid TYPE command. The current data transfer type is for a DBCS data type, but an internal error occurred and the current data type is no longer valid.

System action

The FTP connection with the client ends.

User response

Reconnect to the FTP server and issue the desired TYPE command. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands. If this reply is received repeatedly, make a note of the last few FTP commands you have issued that cause this result, and contact your system programmer

System programmer response

Contact the IBM Support Center with output from the FTP server trace, if available.

501: Error - existing type invalid

Explanation

The FTP server received an invalid TYPE command. FTP tried to continue with the current data transfer type, but an internal error occurred and the current data type is no longer valid.

System action

The FTP connection with the client ends.

User response

Reconnect to the FTP server and issue the desired TYPE command. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands. If this reply is received

repeatedly, make a note of the last few FTP commands you have issued that cause this result, and contact your system programmer

System programmer response

Contact the IBM Support Center with output from the FTP server trace, if available.

501: Error - existing UCS type invalid

Explanation

The FTP server received an invalid TYPE command. The current data transfer type is for a UCS data type, but an internal error occurred and the current data type is no longer valid.

System action

The FTP connection with the client ends.

User response

Reconnect to the FTP server and issue the desired TYPE command. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands. If this reply is received repeatedly, make a note of the last few FTP commands you have issued that cause this result, and contact your system programmer

System programmer response

Contact the IBM Support Center with output from the FTP server trace, if available.

501: File name too long. Use z/OS UNIX file naming conventions.

Explanation

The LIST or NLST command was entered with a file name that was longer than the z/OS UNIX maximum of 1023 characters.

System action

The LIST or NLST command is rejected.

User response

Reissue the LIST or NLST command with the correct z/OS UNIX file name.

System programmer response

None.

501: Invalid data set name *"dsname"*. Use MVS Dsname conventions.

Explanation

The data set name violates one of the MVS file naming conventions and cannot be used to reference a data set at the server.

System action

The data set is not sent. FTP continues.

User response

Rename the data set in compliance with MVS data set naming conventions. For more information about MVS data set naming conventions, see the z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

501: Invalid data set name. Use MVS Dsname conventions.

Explanation

The command was entered with a data set name, but the data set name did not meet MVS data set name conventions. The data set name must:

- Be no more than 44 characters total
- Each qualifier must be no more than 8 characters total
- Each qualifier must start with a letter or with a dollar sign ($), an at sign (@), or a number sign (#).
- The 2nd–8th characters of each qualifier must be either a letter, a number, or a dollar sign ($), an at sign (@), a number sign (#), a hyphen (-), or a brace (}).

System action

The command is rejected.

User response

Reissue the command with the corrected data set name.

System programmer response

None.

501: Invalid directory name - too large.

Explanation

A command was issued that contained a path name that specified a directory name that was longer than the maximum allowable 44 characters for an MVS data set name, or 1023 characters for a z/OS UNIX file name.

System action

The command is rejected. Control returns to the client for further command processing.

User response

Reissue the command with the corrected path name.

System programmer response

None.

501: Invalid file identifier in RNTO command.

Explanation

The RNTO command was issued to rename a data set or file. The data set (file) identifier is invalid or was not specified.

System action

The data set or file is not renamed. FTP continues.

User response

Reissue the rename command observing the file naming conventions for MVS. For more information about MVS data set naming conventions, see the z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

501: Invalid Jobid

Explanation

A Command was issued requesting JES to delete a job. The job ID was not specified or it was incorrectly specified.

System action

FTP continues.

User response

Reissue the command.

System programmer response

None.

501: Invalid user name '*' in USER command

Explanation

The client attempted to log on to the FTP server with a user ID of *. This is an incorrect user ID.

System action

The user login is rejected. Control returns to the client for further command processing.

User response

Reissue the USER command with the correct user ID.

System programmer response

None.

501: Member name too long. Use MVS naming conventions.

Explanation

The LIST or NLST command was entered with a data set name and member name requested, but the member name was longer than the MVS maximum length of 8 characters.

System action

The LIST or NLST command is rejected.

User response

Reissue the command with the correct member name syntax.

System programmer response

None.

501: Mismatched quotes on directory name "*pathname*".

Explanation

A command was issued that started the path name with a single quote while QUOTESOVERRIDE was TRUE. The FTP server expected a matching ending quote to be found at the end of the path name, but no matching ending quote was found.

System action

The command is rejected. Control returns to the client for further command processing.

User response

Reissue the command with the corrected path name.

System programmer response

None.

501: MKDIR fails: *reason*

Explanation

The MKD command was issued to create a new MVS PDS or a new z/OS UNIX directory, but the path name specified contained only quotation marks with no data set name, had an z/OS UNIX name larger than 1023 characters, or an MVS data set name longer than 44 characters.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Reissue the command with the data set name for the new PDS.

System programmer response

None.

501: No directory name entered

Explanation

The MKD command was entered to create a directory, or the RMD command was entered to delete a directory, but no directory was specified with the command.

System action

The command is rejected. Control returns to the client for further command processing.

User response

Reissue the MKD or RMD command, specifying a valid directory to be created or be deleted.

System programmer response

None.

501: Nonexistent GDG data set *dsname*

Explanation

The relative generation number for the Generation Data Group (GDG) data set is invalid. The number should be a negative integer, a positive integer (for a store command only), or a 0, enclosed in parentheses.

System action

FTP continues.

User response

Reissue the command with a valid relative number for the data set.

System programmer response

None.

501: One or more parameters missing from command *command*

Explanation

The server received a command from the client that was missing one or more parameters.

command is the command that was missing the expected parameters.

System action

The server rejects command *command*. FTP continues processing.

User response

Report the error to the FTP client system programmer.

System programmer response

If the faulty command was generated as a result of incorrect parameters specified by the user, have the user execute the command again using correct parameters. If the faulty command was generated by the client software, report the error to the provider of the client software.

501: Partitioned data set may not be created within a partitioned data set

Explanation

The MKD command was entered to create a new PDS. The *pathname* parameter was not in quotation marks, indicating that the path name should be appended to the current working directory; however, the current working directory was a partitioned data set, and a new partitioned data set cannot be created within the current working directory.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Either issue the CWD command to change the current working directory to a high-level qualifier rather than a PDS and then reissue the MKD command as before, or reissue the MKD command with the path name in quotation marks to prevent appending to the current working directory.

System programmer response

None.

501: Partitioned data set may not be deleted within a partitioned data set

Explanation

The RMD command was issued to delete a PDS. The path name specified with the RMD command was not in quotation marks, indicating that the path name should be appended to the current working directory to determine the name of the PDS to be deleted, but the current working directory was already a PDS and could not be appended to the path name.

System action

The RMD command is rejected. Control returns to the client for further command processing.

User response

Either issue a CWD command to change to current working directory and then issue the RMD command as before, or issue the RMD command with the fully qualified data set name in quotation marks to prevent the current working directory from being appended.

System programmer response

None.

501: password missing from PASS command

Explanation

The PASS command was issued to complete user log on, but no password or password phrase was entered with the PASS command.

System action

Login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Reissue the USER and PASS commands, specifying a password or password phrase with the PASS command.

System programmer response

None.

501: Pathname required with null working directory

Explanation

The LIST (DIR) or NLST (LS) command was entered with a blank path name and the current working directory is null.

System action

FTP continues.

User response

If a listing of data sets is desired, enter a path name with the command.

System programmer response

None.

501: Patterns (% and *) may only be specified in the last qualifier when in directory mode

Explanation

The LIST or NLST command was entered with a path name that contained the global file-name characters % and *. The global file-name characters were not in the last qualifier of the path name, and the MVS server was currently in directory mode. The global file-name characters can only be used in the last qualifier when the server is in directory mode.

System action

The LIST or NLST command is rejected.

User response

Either correct the path name to have the global file-name characters in the last qualifier and reissue the command in directory mode, or issue the SITE DATASETMODE command to change the server to data set mode and then reissue the LIST or NLST command as is.

System programmer response

None.

501: Protection buffer size value is not valid

Explanation

The server received a PBSZ specifying an invalid protection buffer size. The size must be a positive integer in the range of 512–32768.

System action

The command fails. FTP continues.

User response

Reissue the PBSZ command with a valid size.

System programmer response

None.

501: Qualifier too long. Use MVS naming conventions.

Explanation

A LIST or NLST command was entered with a data set name that contained a qualifier that was longer than the MVS maximum of 8 characters.

System action

The LIST or NLST command is rejected.

User response

Correct the data set name and reissue the command.

System programmer response

None.

501: RMDIR fails: *reason*

Explanation

The RMD command was issued to delete a PDS or a z/OS UNIX directory, but the name contained only a set of quotation marks, no data set name, a z/OS UNIX directory longer than 1023 characters, or an MVS data set longer than 44 characters.

System action

The RMD command is rejected. Control returns to the client for further command processing.

User response

Reissue the RMD command with the correct data set name.

System programmer response

None.

501: Store unique not supported for GDG data sets.

Explanation

The method of storing cannot be "store unique" when storing data in a Generation Data Group data set.

System action

FTP continues.

User response

Reissue the command after changing the storing method from store unique.

System programmer response

None.

501: syntax error -- command required for OPTS

Explanation

The server received an OPTS command from the client, but the OPTS command was not syntactically correct. See RFC 2389 for more information about the OPTS command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System action

The OPTS command is ignored. Processing continues.

User response

Issue the command again using the correct syntax.

System programmer response

None.

501: Syntax error -- marker required for REST.

Explanation

A restart (REST) command was received by the FTP server and there was no server marker at which the file transfer is to be restarted. The REST command must have a marker that is coordinated within the client program for a restart to occur.

Note: The REST command should not be issued directly by the user.

System action

FTP continues.

User response

None.

System programmer response

Determine why the client program did not send the marker.

501: syntax error -- pathname *pathname* not allowed for working directory *directory*

Explanation

The FTP server received an XFIF command. The XFIF command is a z/OS FTP proprietary command that directs the server to create a named pipe. The XFIF pathname parameter is a relative path name, and the current working directory is not a z/OS UNIX file system directory. Named pipes are supported only in the z/OS UNIX file system.

See the path and path name information in z/OS UNIX System Services User's Guide for information about absolute path names, relative path names, and the z/OS UNIX file system. See the information about working with directories on the remote host in z/OS Communications Server: IP User's Guide and Commands for information about the working directory.

In the message text:

pathname
The relative path name of the named pipe.

directory
The working directory.

Example

```
Command:
cd 'USER1'
>>> CWD 'USER1'
250 "USER1." is the working directory name prefix.
Command:
mkfifo make.this.named.pipe
>>> xfif make.this.named.pipe
501 syntax error -- pathname make.this.named.pipe not allowed for working directory
USER1.
Command:
```

System action

The FTP server rejects the command.

User response

Do one of the following actions:

- Change the working directory to a z/OS UNIX file system directory, and send the XFIF command to the server again.
- Send a new XFIF command to the FTP server, specifying the named pipe as an absolute path name in the z/OS UNIX file system.

System programmer response

None.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

501: syntax error -- pathname required for *command*

Explanation

The command specified was received with no name specified.

System action

FTP continues.

User response

Reissue the command with a name.

System programmer response

None.

501: too many bad passwords entered, PASS command disabled

Explanation

The PASS command was issued to complete log on to a user ID on the server system, but previous attempts to log in to this user ID with the incorrect password or password phrase have caused the user ID to be locked out and log on for this user ID is no longer allowed.

System action

Login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

The FTP session must end and reconnected to reset the number of bad password or password phrase attempts for the user ID.

System programmer response

None.

501: TYPE command contains invalid parameter

Explanation

A TYPE B command was issued, but one or more of the parameters specifying DBCS options is invalid or a TYPE U command was issued, but the big/little endian option was invalid.

System action

The TYPE command is rejected. Control returns to the client for further command processing.

User response

Reissue the TYPE command with corrected parameters. See z/OS Communications Server: IP User's Guide and Commands for information on the parameters for the TYPE subcommand.

System programmer response

None.

501: TYPE command syntax error: *num* parameter invalid

Explanation

The TYPE command was issued by the client. The TYPE command should have the syntax TYPE *type {format opt1 opt2 opt3}* where each parameter is a single character. The FTP server determined that the value entered for parameter specified was not a single character. See the z/OS Communications Server: IP User's Guide and Commands for information about transferring data using the file transfer protocol and the parameters of the TYPE command.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

Re-issue the TYPE command with the correct syntax.

System programmer response

None.

501: TYPE command syntax error: *reason*

Explanation

The TYPE command was issued by the client. The TYPE command should have the syntax TYPE *type {format opt1 opt2 opt3}* where each parameter is a single character. The FTP server determined that for the reason given was not a single character. See the z/OS Communications Server: IP User's Guide and Commands for information about transferring data using the file transfer protocol and the parameters of the TYPE command.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

Re-issue the TYPE command with the correct syntax.

System programmer response

None.

501: Type remains *type*

Explanation

The FTP server received an invalid TYPE command. The current data transfer type remains the type specified.

System action

The FTP transfer data type is unchanged. Control returns to the client for further commands.

User response

If you want to change the data transfer type, reissue the TYPE command with corrected parameters. See the z/OS Communications Server: IP User's Guide and Commands for information about valid TYPE parameters.

System programmer response

None.

501-: Unknown mode *new_mode*

501: Data transfer mode remains *old_mode*

Explanation

The MODE command was entered to change the setting of MODE to *new_mode*; but *new_mode* was not a valid mode value.

System action

The MODE command is rejected and control returns to the client for further command processing.

User response

Reissue the MODE command with a valid value. Valid values are S (stream), B (block), or C (compressed).

System programmer response

None.

501-: Unknown structure *new_stru*

501: Data structure remains *old_stru*

Explanation

The STRU command was entered to change the structure to *new_stru*, but *new_stru* was not a valid setting for the structure.

System action

The STRU command is rejected. Control returns to the client for further command processing.

User response

Reissue the STRU command with a valid value. Valid values are R (record structure) and F (file structure).

System programmer response

None.

501-: unknown type *type_value*

Explanation

The client entered the TYPE command to change the type setting to *type_value*, but the server did not recognize the *type_value* as a valid setting for TYPE.

System action

The TYPE command is rejected. Control returns to the client for further commands.

User response

Reissue the TYPE command with a valid TYPE value. For information about valid TYPE values, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

501: User name missing from USER command

Explanation

The client attempted to log on to the FTP server, but the name of the user ID to be logged in was missing from the USER command.

System action

The user login is rejected. Control returns to the client for further command processing.

User response

Reissue the USER command with the appropriate user ID.

System programmer response

None.

501: Wildcards not allowed in PDS name

Explanation

The LIST or NLST command was issued requesting that members of a partitioned data set be listed. The name of the PDS contained one or more global file-name characters * or %. When listing members of a PDS, global file-name characters are allowed only in the member name, not in the PDS name.

System action

The LIST or NLST command is rejected.

User response

Correct the data set name and reissue the request.

System programmer response

None.

502 reply codes

502: command aborted -- server not configured for LANG

Explanation

The server received a LANG command, but the server is not configured to support LANG.

System action

The LANG command is ignored. Processing continues.

User response

Report the error to the administrator of the FTP server.

System programmer response

If you want the server to support the LANG command, code EXTENSIONS UTF8 in the server's FTP.DATA file. See the z/OS Communications Server: IP Configuration Reference for more information about the EXTENSIONS statement.

502: command aborted -- UTF-8 translation not available

Explanation

The server received a command that cannot be supported unless UTF-8 translation is available to the server. The server has been configured for UTF-8 support, but the translation is not available. Either z/OS is not configured to support translation between the host page and UTF-8, or UTF-8 encoding has been disabled for this session. Any SITE command that affects the encoding of the control connection will disable UTF-8 for the remainder of the FTP session. See the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

System action

Processing continues.

User response

Report the error to the system programmer.

System programmer response

Inspect SYSLOG output to determine whether the error is due to z/OS setup, or to the user issuing SITE commands that affect encoding on the control connection. See the z/OS Communications Server: IP Configuration Guide for more information about enabling UTF-8 encoding on the control connection, and the z/OS Communications Server: IP User's Guide and Commands for information about the SIte subcommand.

502: command *command* not implemented

Explanation

The client entered the FTP command *command*, but the FTP server does not support this command.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

None.

System programmer response

None.

502: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

502: error in host address

Explanation

The PORT command was issued by the client. When parsing the PORT command, the FTP server found an error.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

If the command was issued by the user, reissue the command with the correct syntax. If the command was issued automatically by the FTP client, contact the owner of the FTP client program for a possible programming error.

System programmer response

None.

502: error in host address '*value*'

Explanation

The server received one of these commands containing a port number: EPRT or PORT.

value is the value of the port number parameter. The port number parameter is not valid.

The PORT command was issued by the client. The PORT command should have the syntax PORT *h1, h2, h3, h4, p1, p2* where *h1—h4* are integers that make up the host address and *p1* and *p2* are integers that make up the port address. When parsing the PORT command, the FTP server found a nonnumeric character in one of the 4 integers that make up the host address.

The EPRT command should have the syntax EPRT <d><net-prt><d><net-addr><d><tcp-port> where:

<d>
is a delimiter character.

<net-prt>
is the network protocol.

<net-addr>
is the network address.

<tcp-port>
is the port number.

When parsing the EPRT command, the FTP server could not parse the *tcp-port* parameter.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

If the command was issued by the user, reissue the command with the correct syntax. If the command was issued automatically by the FTP client program, contact the owner of the FTP client program for a possible programming error in the client program.

System programmer response

None.

502: error in port number

Explanation

The PORT command was issued by the client. When parsing the PORT command, the FTP server found an error.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

If the command was issued by the user, reissue the command with the correct syntax. If the command was issued automatically by the FTP client, contact the owner of the FTP client program for a possible programming error.

System programmer response

None.

502: error in port number '*value*'

Explanation

The server received one of these commands containing a port number: EPRT or PORT.

value is the value of the port number parameter. The port number parameter is not valid.

The PORT command was issued by the client. The PORT command should have the syntax PORT *h1,h2,h3,h4,p1,p2* where *h1—h4* are integers that make up the host address and *p1* and *p2* are integers that make up the port address. When parsing the PORT command, the FTP server found a nonnumeric character in one of the 2 integers that make up the port address.

The EPRT command should have the syntax EPRT <d><net-prt><d><net-addr><d><tcp-port> where:

<d>
is a delimiter character.

<net-prt>
is the network protocol.

<net-addr>
is the network address.

<tcp-port>
is the port number.

When parsing the EPRT command, the FTP server could not parse the *tcp-port* parameter.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

If the command was issued by the user, reissue the command with the correct syntax. If the command was issued automatically by the FTP client program, contact the owner of the FTP client program for a possible programming error in the client program.

System programmer response

None.

502: error parsing *command_name* command

Explanation

The client sent a command to the FTP server. An error occurred when the FTP server attempted to parse the command and its arguments.

command_name is the name of the command that could not be parsed.

System action

The server rejects the *command_name* command.

User response

Report the error to the system programmer.

System programmer response

Inspect the command that the server rejected. If the command is syntactically valid, activate the FTP server trace, re-create the problem, save the system log for problem determination, and report the problem to IBM. Otherwise, report the error to the provider of the FTP client software.

502: PORT command syntax error - insufficient digits in host-port

Explanation

The PORT command was issued by the client. The PORT command should have the syntax PORT *h1,h2,h3,h4,p1,p2* where *h1—h4* are the 4 integers that make up the host address and *p1* and *p2* are the 2 integers that make up the port address. When parsing the PORT command, the FTP server did not find a total of 6 integer values to make up the host address and port address.

System action

The command is rejected. Control is returned to the client for further command processing.

User response

If the command was issued by the user, reissue the command with the correct syntax. If the command was issued automatically by the FTP client program, contact the owner of the FTP client program for a possible programming error in the client program.

System programmer response

None.

503 reply codes

503 : Authentication already established

Explanation

The server received an ADAT command but authentication has already been successfully negotiated.

System action

The command fails. FTP continues.

User response

None.

System programmer response

None.

503: Command *command* rejected - *command* not allowed after *prior_command* command

Explanation

The FTP client sent a command to the server. The server rejected the command because the command is not compatible with a command that the client sent to the server earlier in the login session.

In the reply text:

command
The command that the server rejected. This command is incompatible with the command specified by the *prior_command* value.

prior_command
The command that the client sent earlier in the session. This command is incompatible with the command specified by the *prior_command* value.

Example

```
503 Command PROT rejected -- PROT not allowed after CCC
```

System action

The FTP server ignores the specified command.

User response

Contact the system programmer.

System programmer response

If the *prior_command* value is CCC, it is probable that the user violated the rules established in RFC 4217 for using a TLS-secured session. When the control connection has been cleared, RFC 4217 stipulates that the server must reject certain commands. See RFC 2228 *FTP Security Extensions* and RFC 4217 *Securing FTP with TLS* for more information about the correct sequencing of commands during a secured session. Educate the user in the correct use of a secured session. If the *prior_command* value is not CCC, see RFC 959 *File Transfer Protocol* for information about correct command sequences during an FTP session. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

503: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

503: EPSV ALL received - *command* not allowed after EPSV ALL

Explanation

The client sent *command* to the server. Previously during the login session, the client sent an EPSV ALL command to the server. *command* is not allowed after an EPSV ALL command has been sent to the server.

System action

FTP rejects *command*. The FTP server continues processing commands from the client.

User response

If you must use *command*, exit the current session and log in to the FTP server again. Do not issue EPSV ALL before issuing *command*.

System programmer response

None.

503 : Must first establish authentication

Explanation

The server received a command that is not valid unless the client and server successfully negotiated authentication, but authentication was not successfully negotiated.

System action

The command fails. FTP continues.

User response

Issue an AUTH command and reissue the failing command. See RFC 2228 for more information about the OPTS command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System programmer response

None.

503 : Must first issue PBSZ

Explanation

The server received a command that is not valid unless a PBSZ command was previously received, but a PBSZ command was not received.

System action

The command fails. FTP continues.

User response

Issue a PBSZ command and reissue the failing command. See RFC 2228 for more information about the OPTS command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System programmer response

None.

503 : Must issue AUTH command before ADAT command

Explanation

The server received an ADAT command but had not previously received an AUTH command. An AUTH command must always precede an ADAT command.

System action

The command fails. FTP continues.

User response

Issue an AUTH command and reissue the ADAT command. See RFC 2228 for more information about the OPTS command. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

System programmer response

None.

503: PASS command must be preceded by USER

Explanation

The PASS command was entered to complete log on of a user ID on the server system, but the USER command has not been issued to specify which user ID to log in to. The USER command must be issued to specify the user ID before the PASS command can be issued.

System action

Login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Issue the USER command to specify the user ID of the server system to log in to, then reissue the PASS command with the password or password phrase for this user ID.

System programmer response

None.

503 : Server on the TLS secure port does not accept the AUTH command

Explanation

The FTP client program connected to an FTP server that is running on the TLS secure port 990. The FTP server assumes that all connections are protected by the TLS security mechanism and that an AUTH command is not needed to initiate a TLS handshake.

System action

FTP continues.

User response

Close the connection to the FTP server and reconnect without sending an AUTH command.

System programmer response

None.

504 reply codes

504: Block mode not implemented for type B.

Explanation

The data type B (double Byte) is not supported while in block transmission mode.

System action

FTP continues.

User response

Either change to mode s (stream) or change the data type to EBCDIC and reissue the command.

System programmer response

None.

504: Command *command* aborted -- FTP server not configured for parameter *parameter*.

Explanation

The client issued a command to the FTP server. The FTP server implements the command but is configured to reject commands with the specified parameter.

command is the command the client sent to the server.

parameter is the *command* parameter rejected by the server.

When *command* is EPRT, the PORTCOMMANDPORT or PORTCOMMANDIPADDR statement in FTP.DATA is coded to reject *parameter*.

System action

The command is rejected.

User response

Report the error to the FTP server installation system programmer.

System programmer response

If you want your FTP server to support the combination of *command* and *parameter* , code statements in FTP.DATA to enable this support. See the z/OS Communications Server: IP Configuration Reference for information about enabling *command* and *parameter* support for your FTP server.

504: command *command* into named pipe fails -- filetype must be SEQ

Explanation

The server received the specified command while UNIXFILETYPE=FIFO was configured. The UNIXFILETYPE value must be SEQ to transfer data into a named pipe.

For more information, see the following topics:

- The information about using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User's Guide and Commands.
- The information about UNIXFILETYPE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference.
- The information about FILETYPE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference.

In the message text:

command
The command that the server received.

Example

```
Command:
site unixfiletype=fifo filetype=sql
>>> SITE unixfiletype=fifo filetype=sql
200 SITE command was accepted
Command:
put /tmp/notfifo  /tmp/sample.fifo
>>> PORT 9,42,105,36,4,49
200 Port request OK.
>>> STOR /tmp/sample.fifo
504 command STOR into named pipe fails - filetype must be SEQ
Confidence=Low for PUT of /tmp/notfifo
Command:
```

System action

The FTP server rejects the command.

User response

Use the SITE command to change either the UNIXFILETYPE value or the FILETYPE value, and transfer the file again.

- From the z/OS FTP client, issue the SIte subcommand with the UNIXFILETYPE or FILETYPE parameter.
- From any FTP client, issue the QUOTE subcommand, specifying a SITE command with the UNIXFILETYPE or FILETYPE parameter.

See the information about the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

504: command STOU not supported for named pipes

Explanation

The FTP server received a STOU (store-unique) command that specified a named pipe. The command is not supported for named pipes.

The UNIXFILETYPE configuration option at the FTP server determines whether the STOU command argument is a named pipe or a regular z/OS UNIX file. See the UNIXFILETYPE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference for more information about the UNIXFILETYPE configuration option.

See the information about using z/OS UNIX System Services named pipes in z/OS Communications Server: IP User's Guide and Commands for information about transferring data to named pipes..

Example

```
Command:
put /etc/hosts /tmp/my.fifo
>>> PORT 9,2,1,3,4,44
```

```
200 Port request OK.
>>> STOU /tmp/my.fifo
504 command STOU not supported for named pipes
Command:
```

System action

The FTP server rejects the STOU command.

User response

Do one of the following actions:

- Append to the named pipe instead of storing into the named pipe.
- Configure your FTP client to send the STOR command instead of the STOU command to the server, and send the file or data set again. See the SUnique subcommand in z/OS Communications Server: IP User's Guide and Commands for information about configuring the z/OS FTP client to send the STOR command instead of the STOU command.

System programmer response

None.

Problem determination

See the user response.

Source

z/OS Communications Server TCP/IP: FTP

504: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

504: Compress mode not implemented for type B.

Explanation

The data type B (double Byte) is not supported while in compress transmission mode.

System action

FTP continues.

User response

Either change to mode s (stream) or change the data type to EBCDIC and reissue the command.

System programmer response

None.

504: Data structure remains *old_stru*

Explanation

The STRU command was entered to change the structure to PAGE, but PAGE structure is not supported by the FTP server.

System action

The STRU command is rejected. Control returns to the client for further command processing.

User response

Reissue the STRU command with a valid value. Valid values are R (record structure) and F (file structure).

System programmer response

None.

504: Error - existing kanji type invalid

Explanation

The FTP server received an invalid TYPE command. The current data transfer type is for a DBCS data type, but an internal error occurred and the current data type is no longer valid.

System action

The FTP connection with the client ends.

User response

Reconnect to the FTP server and issue the desired TYPE command. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands. If this reply is received repeatedly, make a note of the last few FTP commands you have issued that cause this result, and contact your system programmer

System programmer response

Contact the IBM Support Center with output from the FTP server trace, if available.

504: Error - existing type invalid

Explanation

The FTP server received an invalid TYPE command. FTP tried to continue with the current data transfer type, but an internal error occurred and the current data type is no longer valid.

System action

The FTP connection with the client ends.

User response

Reconnect to the FTP server and issue the desired TYPE command. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands. If this reply is received repeatedly, make a note of the last few FTP commands you have issued that cause this result, and contact your system programmer

System programmer response

Contact the IBM Support Center with output from the FTP server trace, if available.

504: Filetype SQL requires type A (ASCII) or E (EBCDIC) or B (DBCS)

Explanation

The FTP server received a request to transfer a file. The current FTP filetype is SQL, and the current data transfer type is neither ASCII (A) nor EBCDIC (E).

System action

FTP continues.

User response

From the FTP client, change either the current filetype or the current data transfer mode. For information on changing the filetype and data transfer mode for the z/OS client, see the z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

504: Lrecl X transfer not supported with *condition*

Explanation

A GET was issued for a data set with lrecl X and an incorrect condition was detected.

condition is one of the following values:

- MODE C — Compressed Mode.
- TYPE U 2 — Data type U 2.
- FILETYPE=SQL — SQL.
- NOASATRANS — NOASAtrans cannot be specified with lrecl X w/ASA.
- STRUCT R — Record structure.

System action

The request is rejected. FTP continues.

User response

Retrieve the lrecl X data set using the correct FILETYPE, MODE, STRUCT, TYPE, or ASATRANS setting.

System programmer response

None.

504: Lrecl X transfer not supported with Record I/O

Explanation

A GET was issued for a data set with lrecl X and Record I/O was requested. The condition is unexpected.

System action

The request is rejected. FTP continues.

User response

Contact your system programmer.

System programmer response

Collect an FTP Server trace that includes the failure and call the IBM Support Center.

504: NOASATRANS is not supported for TYPE U. Use 'SITE ASATRANS'

Explanation

You attempted to get a data set when ASA control characters were being converted to C control characters and the transfer type is Unicode.

System action

The request is rejected. FTP continues.

User response

Turn on ASA control character transfer (SITE ASATRANS)

System programmer response

None.

504: Only local byte size allowed is 8

Explanation

The client entered the TYPE command with a parameter of “L byte_size” to change the type setting to the specified local byte size. The byte_size specified by the command was a value other than 8, but the only local byte size supported by the server is 8.

System action

The TYPE command is rejected. Control returns to the client for further commands.

User response

Reissue the TYPE command with a valid local byte size.

System programmer response

None.

504-: Only 'TYPE U 2' is supported

Explanation

The client entered the TYPE command in the format “TYPE type_value *format*” to change the type setting, but the *format* specified was not recognized by the FTP server.

System action

The TYPE command is rejected. Control returns to the client for further command processing.

User response

Reissue the TYPE command with a valid format value. For information about valid parameters for the TYPE command, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

504-: Page structure not implemented

Explanation

The STRU command was entered to change the structure to PAGE, but PAGE structure is not supported by the FTP server.

System action

The STRU command is rejected. Control returns to the client for further command processing.

User response

Reissue the STRU command with a valid value. Valid values are R (record structure) and F (file structure).

System programmer response

None.

504: parameter *parameter* not supported

Explanation

The server received a command with a parameter, *parameter*, it does not support.

System action

FTP continues.

User response

Issue the command again with a valid parameter.

System programmer response

None.

504: Port command not implemented for that parameter

Explanation

User attempted port command using incorrect parameters.

The FTP client sent a PORT command to the server. The server is configured to reject PORT commands with the parameter that you specified.

System action

The request is rejected. FTP continues.

User response

Contact system programmer.

System programmer response

See the z/OS Communications Server: IP Configuration Reference for information about configuring your server to reject PORT commands with the PORTCOMMAND, PORTCOMMANDIPADDR, and PORTCOMMANDPORT statements. Correct the server configuration as appropriate for your installation. Advise users of any restrictions you have placed on the PORT command parameters.

504: Record structure is not supported for TYPE U transfer

Explanation

You attempted to get a data set while the data structure is defined as Record and the transfer type is Unicode.

System action

The request is rejected. FTP continues.

User response

Change the data structure to File (STRUCT F)

System programmer response

None.

504: Restart not allowed for named pipes

Explanation

The FTP server received a REST (restart) command from the FTP client as part of a sequence of commands to transfer data to the FTP server. The REST command instructs the server that the current file transfer is a resumption of an interrupted file transfer. The server file is a named pipe. File transfer to a named pipe cannot be restarted.

Example

```
>>> rest 10
350 REST command accepted, parameter 10.
>>> PORT 9,2,1,3,4,43
200 Port request OK.
>>> STOR /tmp/my.fifo
504 Restart not allowed for named pipes.
Command:
```

System action

The FTP server rejects the file transfer.

User response

Notify the system programmer.

System programmer response

If the server application that reads from the named pipe can tolerate reading the same data more than once from the named pipe, instruct the user to transfer the entire file to the named pipe again instead of attempting to restart the file transfer.

Otherwise, identify the last data read by the server application, and provide a new file or data set to the FTP client starting from that point. Have the user transfer the new file or data to the named pipe.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

504 : Restart not allowed with active security mechanism

Explanation

The connection to the FTP server is protected by a security mechanism (for example, TLS). While the connection is protected, the restart of a failed data transfer is not allowed.

System action

FTP continues.

User response

Possible responses can be the following ones:

- Reissue the data transfer command to transfer all of the data of file.
- Close the connection, reconnect without a security mechanism in place, and then issue the restart command.

System programmer response

None.

504: restart is not supported for type *type*

Explanation

You attempted to restart a data transfer command. Restart is not supported for the current data type.

type is the current data type setting.

System action

The data transfer is not resumed. FTP continues.

User response

If *type* was the data type in use during the file transfer you want to resume, you will not be able to resume the file transfer. Issue the original data transfer command to transmit the file. Otherwise, set the data type to the value in effect during the file transfer you want to resume; then try to restart the data transfer.

System programmer response

None.

504: Restart not allowed for store unique.

Explanation

A restart (REST) command was received by the FTP server and the storage method is "store unique." This combination is not allowed for a restarted store operation.

System action

FTP continues.

User response

Change from store unique method and reissue the restart command.

System programmer response

None.

504: Restart requires Block or Compressed transfer mode.

Explanation

You attempted to restart a checkpointed data transfer command and the transfer mode is not block or compressed.

System action

The data transfer command is not restarted. FTP continues.

User response

Change the transfer mode to block or compressed and re-issue the restart command.

System programmer response

None.

504: Restart requires EBCDIC data type.

Explanation

You attempted to restart a checkpointed data transfer command and the data type is not EBCDIC.

System action

The data transfer command is not restarted. FTP continues.

User response

Change the data type to EBCDIC and re-issue the restart command.

System programmer response

None.

504: Restart requires filetype=SEQ.

Explanation

You attempted to restart a checkpointed data transfer command and the filetype is not SEQ.

System action

The data transfer command is not restarted. FTP continues.

User response

Change the filetype to SEQ and re-issue the restart command.

System programmer response

None.

504 : Server does not understand the specified mechanism

Explanation

The AUTH command specified a security mechanism name that is too long for the FTP server to process. The security mechanism names supported by the FTP server are GSSAPI and TLS. TLS support can also be requested with a mechanism name of TLS-C, TLS-P, or SSL.

System action

FTP continues.

User response

Reissue the AUTH command with one of the supported security mechanism names.

System programmer response

None

504 : Server does not understand the specified protection level

Explanation

The PROT command has requested a data protection level that is unknown to the FTP server. The request to set the level is rejected. The level specified on the command must be one character long. The following list shows the valid level names:

C
Clear

P
Private

S
Safe

System action

FTP continues.

User response

Reissue the PROT command with one of the valid level names.

System programmer response

None.

504: Server SBSENDEOL must be CRLF for SIZE command

Explanation

The server sends this reply when it receives a SIZE command while SBSENDEOL is not set to CRLF. FTP cannot reliably calculate the file transfer size when the SBSENDEOL setting is not CRLF.

System action

The SIZE command is rejected.

User response

If you want to change the setting of SBSENDEOL for this session, use the SITE SBSENDEOL=*value* subcommand. See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information. If you continue to experience this error, report the error to the system programmer.

System programmer response

Most clients do not require or tolerate an SBSENDEOL setting other than CRLF. If your users require the alternate server SBSENDEOL setting only for certain file transfers, code SBSENDEOL CRLF in the server's FTP.DATA and instruct your users to send a SITE SBSENDEOL command to the server just before those file transfers. The server will accept the SIZE command until the SBSENDEOL value is reset.

The SIZE command is often part of a sequence of commands sent by the FTP client to restart a file transfer while in stream mode. If your users often need to restart file transfers, consider whether block or compressed mode transfers would be appropriate for your installation. Block and compressed mode transfers can be restarted provided you have initiated checkpointing before the file transfer. See the information about restarting a failed data transfer in z/OS Communications Server: IP User's Guide and Commands for more information.

504: Server SBSENDEOL must be CRLF for stream mode restart of RETR command

Explanation

The server sends this reply to the client when all these conditions are true:

- The type is ASCII and the mode is STREAM.
- The SBSENDEOL setting is not CRLF.
- The server has just processed a REST command while type is ASCII and mode is STREAM.
- The server is now processing a RETR command.

The server rejects the RETR command with this reply when the FTP client is trying to restart a file retrieve transfer in stream mode. For z/OS FTP client users, the client tries to restart a file retrieve when the user issues an **srestart get** subcommand. Stream mode restart of file retrieve is not supported by the z/OS FTP server when the SBSENDEOL setting has been changed from CRLF.

System action

The RETR command is rejected by the server.

User response

You must transfer the file again in its entirety instead of restarting the file transfer. If you continue to experience this error, report the error to the system programmer.

System programmer response

Most clients and servers do not tolerate an SBSENDEOL setting other than the default, CRLF. When you code SBSENDEOL as a different value in the server's FTP.DATA, or send a SITE SBSENDEOL command to the server to set the value to anything besides CRLF, your users will not be able to restart a file retrieve in stream mode. If your installation requires the alternate server SBSENDEOL setting for only certain file transfers, code SBSENDEOL CRLF in the server's FTP.DATA and instruct your users to send a SITE SBSENDEOL command to the server just prior to those file transfers. The users will be able to restart stream mode file transfers that are interrupted before resetting SBSENDEOL.

Advise your users not to trick the FTP server into restarting a file retrieve that failed while the server's SBSENDEOL value was not CRLF because the result will likely be corrupted files.

Also, consider whether block or compressed mode file transfers would be appropriate for your installation. Block mode transfers can be restarted, provided you have initiated checkpointing before the file transfer. See the information about restarting a failed data transfer in z/OS Communications Server: IP User's Guide and Commands for more information.

504: STAT file-identifier: not implemented

Explanation

The STAT subcommand was entered with the file-identifier parameter. The file-identifier parameter of the STAT subcommand is not supported by the FTP server.

System action

FTP continues.

User response

None.

System programmer response

None.

504: Stream mode restart not supported for MVS data sets

Explanation

The FTP server received a request to restart transmission of an MVS data set. The current data transmission mode is Stream. Stream mode restart is not supported for MVS data sets.

System action

The restart request is ignored. Processing continues.

User response

If stream mode was in use during the file transfer you want to resume, you will not be able to resume the file transfer. Issue the original data transfer command to transmit the file. Otherwise, set the mode to the value in effect during the file transfer you want to resume; then try to restart the data transfer.

System programmer response

None.

504: Struct R implemented with stream mode only.

Explanation

You attempted to get or store a data set while the data structure is defined as record and the transfer mode is not stream mode.

System action

The request is rejected. FTP continues.

User response

Change the transfer mode to stream (MODE S) or change the data structure to file (STRU F).

System programmer response

None.

504: SUBSYS parameter not supported for APPE command

Explanation

You tried to append to a server file while the SUBSYS parameter was configured. Appending to a server file is not supported when the SUBSYS option is configured.

Example

```
ftp> type I
ftp> site subsys=bp01
ftp> append 'user.data' 'user.output'
504 SUBSYS parameter not supported for APPE command
```

System action

The file transfer fails.

Operator response

Not applicable.

User response

If you intended to use the SUBSYS parameter, and your client is the z/OS FTP client, use the PUT subcommand instead of the APPEND subcommand to send the file to the server. Otherwise, send a SITE command that specifies the SUBSYS parameter without a subsystem name to the FTP server to disable subsystem processing. See the information about the PUT subcommand and the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands .

System programmer response

Not applicable.

Problem determination

Not applicable.

Source

Not applicable.

Module

Not applicable.

Routing code

Not applicable.

Descriptor code

Not applicable.

504: Transfer of RDWs is not supported for TYPE U. Use 'SITE NORDW'

Explanation

You attempted to get a data set while RDWs for variable format data sets were retained as data and the transfer type is Unicode.

System action

The request is rejected. FTP continues.

User response

Change the RDW setting (SITE NORDW)

System programmer response

None.

504: Transfer of trailingblanks is not supported for TYPE U. Use 'SITE NOTRAILINGBLANKS'

Explanation

You attempted to get a data set while trailing blanks were retained for fixed format data set and the transfer type is Unicode.

System action

The request is rejected. FTP continues.

User response

Turn off trailing blanks (SITE NOTRAILINGBLANKS)

System programmer response

None.

504-: TYPE command contains extraneous parameter *parm*

Explanation

The FTP server received an invalid TYPE command. The TYPE command contained too many parameters.

System action

The FTP transfer data type is unchanged. Control returns to the client for further commands.

User response

If you want to change the data transfer type, reissue the TYPE command with corrected TYPE parameters. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

504: Type *format* file transfer is not supported when SUBSYS is configured

Explanation

You issued a SITE command that specified the SUBSYS parameter. Then you attempted a file transfer using a data transfer type other than binary. When SUBSYS is configured, the only supported transfer type is binary. See RFC 959 for information about FTP transfer types. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs.

In the reply text:

format
The transfer type that was specified.

Example

```
ftp> site subsys=BP01
ftp> type A
ftp> put 'user.data'
504 Type A file transfer is not supported when SUBSYS is configured
```

System action

The file transfer fails.

Operator response

Not applicable.

User response

If you intended to use the SUBSYS parameter, change the transfer type to binary. If your client is the z/OS FTP client, see the BINARY subcommand and TYPE subcommand in z/OS Communications Server: IP User's Guide and Commands for information about setting the transfer type. Otherwise, to disable subsystem processing, send a SITE command specifying the SUBSYS parameter with no subsystem name to the FTP server.

System programmer response

Not applicable.

Problem determination

Not applicable.

Source

Not applicable.

Module

Not applicable.

Routing code

Not applicable.

Descriptor code

Not applicable.

504-: TYPE has unknown format *format*

Explanation

The FTP server received an invalid TYPE command. The transfer type shown remains.

System action

The FTP transfer data type is unchanged. Control returns to the client for further commands.

User response

If you want to change the data transfer type, reissue the TYPE command with corrected TYPE parameters. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

504-: TYPE has unsupported format *format*

Explanation

A TYPE A or TYPE E command was received by the FTP server, but format *format* is not supported. The only format parameter supported is N (Non-PrinT), which is also the default.

System action

The TYPE command is rejected. Control returns to the client for further command processing.

User response

Reissue the corrected TYPE command.

System programmer response

None.

504-: TYPE not Supported. Translation table not Loaded.

Explanation

A TYPE B command was received for a DBCS language, but the required DBCS translation table is not available to the FTP server.

System action

The TYPE command is rejected. Control returns to the client for further command processing.

User response

Contact the system programmer at the server system to get the necessary DBCS tables loaded.

System programmer response

Ensure that the TCP/IP.DATA file contains a LOADDBCSTABLES statement that correctly specifies the DBCS languages whose translation tables are to be loaded. For information about the LOADDBCSTABLES parameters, see z/OS Communications Server: IP Configuration Reference. If the TCPIP.DATA file is changed, the FTP server must be restarted to recognize the change.

504-: Type not supported. Unable to load *lang* translation tables.

Explanation

The FTP server received a TYPE B command but an error occurred when the server tried to load the required translation tables for this client.

System action

The TYPE command is rejected. Control returns to the client for further commands.

User response

Contact the system programmer for the FTP server's system.

System programmer response

Look in the system log for the FTP server for message EZY2721E or EZY2722E. Probable causes of the problem include unable to open the file containing the translation tables, insufficient storage available for the translate tables, or the file format is invalid.

504: Type remains *type*

Explanation

The FTP server received an invalid TYPE command. The transfer type shown remains.

System action

The FTP transfer data type is unchanged. Control returns to the client for further commands.

User response

If you want to change the data transfer type, reissue the TYPE command with corrected TYPE parameters. For information about valid TYPE parameters, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

504: TYPE U transfer is not supported for filetype *type*

Explanation

You attempted to get a data set while the file type was not SEQuential and the transfer type was Unicode.

System action

The request is rejected. FTP continues.

User response

Change the file type to SEQuential (SITE FILETYPE=SEQ)

System programmer response

None.

504: TYPE U transfer is not supported in mode *mode*

Explanation

You attempted to get a data set while the transfer type is defined as Unicode and the transfer mode is not stream mode.

System action

The request is rejected. FTP continues.

User response

Change the transfer mode to stream (MODE S)

System programmer response

None.

504: TYPE U transfer is supported only for filetype SEQ

Explanation

You attempted to get a data set while the transfer type is defined as Unicode and the filetype is not sequential.

System action

The request is rejected. FTP continues.

User response

Change the filetype to SEQ (SITE FILETYPE=SEQ)

System programmer response

None.

504: TYPE U transfer is supported only in stream mode

Explanation

You attempted to get a data set while the transfer type is defined as Unicode and the transfer mode is not stream mode.

System action

The request is rejected. FTP continues.

User response

Change the transfer mode to stream (MODE S)

System programmer response

None.

504-: Unable to set up conversion between UCS-2 and *codeset*

Explanation

The FTP server was unable to setup a conversion between UCS-2 and EBCDIC or EBCDIC and UCS-2 when TYPE U 2 was received.

System action

The FTP transfer data type is unchanged. Control returns to the client for further commands.

User response

If you want to change the data transfer type, issue the SITE UCSHOSTCS command to change the EBCDIC code set and reissue the TYPE command. For information about UCSHOSTCS, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

504 : Unknown authentication type *mechname*

Explanation

The AUTH command specified a security mechanism name that is unknown to the FTP server. The security mechanism names supported by the FTP server are GSSAPI and TLS. TLS support can also be requested with a mechanism name of TLS-C, TLS-P, or SSL.

mechname is the name of the security mechanism specified on the AUTH command.

System action

FTP continues.

User response

Reissue the AUTH command with one of the supported security mechanism names.

System programmer response

None.

504: WRAPRECORD is not supported for TYPE U. Use 'SITE NOWRAPRECORD'

Explanation

You attempted to get a data set when record wrapping was on and the transfer type is Unicode.

System action

The request is rejected. FTP continues.

User response

Turn off record wrapping (SITE NOWRAPRECORD)

System programmer response

None.

509 reply codes

509: cannot convert pathname to native character set

Explanation

The server attempted to convert a command received on the control connection to the host character set. The conversion failed. The client might be using an encoding not supported by the FTP server.

System action

The control connection is ended.

User response

Report the error to the administrator of the FTP server.

System programmer response

Inspect the SYSLOG trace for more information about the error.

521 reply codes

521: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

521: *"new_directory"* data set already exists

Explanation

The MKD command was entered to create a new PDS with the name *new_directory*, but a data set with that name already exists at the server system.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Change the name of the *new_directory* to a unique name and reissue the MKD command.

System programmer response

None.

522 reply codes

522: command PORT not allowed with this session - current protocol is not IPv4.

Explanation

The FTP client sent a PORT command to the z/OS FTP server. The PORT command is not appropriate for the current session because the session protocol is not IPv4. The FTP client might send such a command to the server if the user is trying to proxy transfer files between two servers, and the two servers are known to the client by IP addresses of different protocol families. Even a z/OS FTP server with both IPv4 and IPv6 interfaces will not accept a PORT command if the client logged in to that server with an IPv6 IP address.

System action

The FTP server rejects the PORT command. The server waits for the next FTP command.

User response

If you received this reply while attempting a proxy transfer of data between two servers, and the proxy transfer failed subsequent to this reply, try the strategies listed below. If you received this reply under any other circumstance, report the error to the system programmer.

- Log in to the FTP servers as before, but reverse the order in which you log in to those servers. Try the proxy transfer again. The strategy is to reverse the roles of the FTP servers from the client's perspective so that the FTP client sends PORT or EPRT to the other FTP server.

- Log in to each server again by specifying server IP addresses of the same protocol family, and try the proxy transfer again. If you know the servers only by DNS names, ask the system programmer what the server IP addresses are. If both servers are z/OS FTP servers, this is the only way to successfully proxy transfer files.
- If neither of the above strategies succeeds, you cannot proxy transfer files directly between the servers. Transfer the file first to the client, then from the client to the other server.

System programmer response

If the user is attempting proxy transfer between two FTP servers, verify that the user correctly attempted the strategies in the **User or Operator Response**. Otherwise, report the error to the provider of the FTP client software.

522: network protocol *netprt_specified* not consistent with this session. Use *netprt_allowed*.

Explanation

The FTP client sent an EPRT command to the z/OS FTP server to establish a data connection. The network protocol specified on the EPRT command is not allowed for the current session because it is not the same protocol the client used to log in to FTP.

netprt_specified is the network protocol address family number specified on the EPRT command.

netprt_allowed is the network protocol address family number allowed for the current session.

Address family (AF) numbers correspond to protocols supported by the FTP server. The address family numbers are defined in RFC 1700. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs. The FTP server might return one of these values:

AF number
Protocol

1
Internet Protocol Version 4

2
Internet Protocol Version 6

The z/OS FTP server supports both IPv4 and IPv6, but the EPRT command is not allowed to specify a protocol different from that used for the current session. An FTP client may send such a command when the user is attempting proxy transfer between two servers known to the client by IP addresses of different protocol families.

System action

The FTP server rejects the EPRT command. Processing continues.

User response

If you received this reply while attempting a proxy transfer of data between two servers, and the file transfer failed subsequent to this reply, try one of the strategies listed below. If you received this reply under any other circumstance, report the error to the system programmer.

- Log in to the FTP servers as before, but reverse the order in which you log in to those servers. Try the proxy transfer again. The strategy is to reverse the roles of the FTP servers from the client's perspective so that the FTP client sends PORT or EPRT to the other FTP server.
- Log in to each server again by specifying server IP addresses of the same protocol family, and try the proxy transfer again. If you know the servers only by DNS names, ask the system programmer what the server IP addresses are. If both servers are z/OS FTP servers, this is the only way to successfully proxy transfer files.

- If neither of the above strategies succeeds, you cannot proxy transfer files directly between the servers. Transfer the file first to the client, then from the client to the other server.

System programmer response

If the user is attempting proxy transfer, verify that the user correctly attempted the strategies described under **User or Operator Response**. Otherwise, report the error to the provider of the FTP client software.

522: Network protocol not supported. Use (*supported_protocols*)

Explanation

The FTP client sent a command to the FTP server to establish a data connection. The FTP server does not support the network protocol that the FTP client specified.

If you specify a network protocol on the EPSV command, that network protocol must match the protocol used for the control connection.

supported_protocols is an address family number, or a list of address family numbers, corresponding to protocols supported by the FTP server. The address family numbers are defined in RFC 1700. See Appendix A, “Related protocol specifications,” on page 809 for information about accessing RFCs. The FTP server might return one or both of the following values:

Address family number
Protocol

1
Internet Protocol Version 4

2
Internet Protocol Version 6

The FTP server supports connections over both IPv6 and IPv4 connections at once, but the z/OS system configuration might limit its support to only one of them.

System action

The current command is rejected by the FTP server. FTP processing continues.

User response

Issue the commands again, using one of the protocols specified in *supported_protocols*.

System programmer response

None.

522: No IPv4 address available for PASV. Use EPSV.

Explanation

The client sent a PASV command to the FTP server to establish a data connection. An affirmative PASV reply must include the server's local IPv4 address. The server cannot reply affirmatively to PASV because it has no local IPv4 address for the PASV reply.

Some FTP clients recover automatically from this situation by sending an EPSV, EPRT, or PORT command to establish the data connection.

System action

The server rejects the PASV command. The FTP server processing continues.

User response

If the client recovered from the error by using a different command to establish the data connection, no further action is needed. Otherwise, report the error to the system programmer.

System programmer response

Choose one of these solutions:

- Configure the FTP client to use EPSV instead of PASV when establishing a passive data connection.
- Configure the client to use PORT instead of PASV to establish a data connection (the client must have an IPv4 address that is reachable from the FTP server).
- If the server has an IPv4 address and an IPv6 address, specify the server's IPv4 address when logging in to FTP.

If none of these solutions is feasible, report the error to the provider of the FTP client software.

525 reply codes

525: No data is available on the data connection

Explanation

On a store/put operation, the first receive() on the data connection did not return any data. The most common reason for this is that the data connection has been reset.

System action

The transfer is ended. FTP continues.

User response

Contact the system programmer.

System programmer response

Examine an FTP server trace to determine why there is no data available on the data connection.

530 reply codes

530-: A load was done from an uncontrolled library

Explanation

The client entered the PASS command. The __passwd function issued by the FTP server failed, indicating that this function is not supported in an address space where a load was done from an uncontrolled library.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

Ensure that programs being loaded from this address space are defined as program controlled. A corresponding ICH420I message is issued identifying the uncontrolled library where the load was done.

530-: An error occurred in the security product

Explanation

The client entered the USER command to log in to the server. The server is using the client certificate that is passed to the server when a TLS protected session was established to authenticate the user. The client certificate is already defined for another process or the certificate does not meet the required format.

System action

The login to the user ID is rejected.

User response

Contact the system programmer.

System programmer response

Find the certificate in the security product and determine whether it is a valid certificate that is registered (associated) with the user ID that is logging in. The required format for the certificate is defined by the __certificate() function in the z/OS XL C/C++ Runtime Library Reference.

530-: An MVS environmental or internal error occurred

Explanation

The client entered the PASS command. The setgroups function issued by the FTP server failed indicating an MVS environmental or internal error occurred.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

There was a MVS internal error. A previous 530 reply should contain the reason code. This reason code will give further information about the setgroups failure.

530-: Anonymous login with security protected session requires anonymousLevel > 2

Explanation

The connection to the FTP server is protected by a security mechanism. Anonymous logins are supported by the FTP server for protected sessions only when the FTP.DATA file statement ANONYMOUSLEVEL has a parameter that is greater than two.

System action

The anonymous login fails.

User response

Contact the system programmer with the error.

System programmer response

To allow anonymous logins with an active security mechanism, give the ANONYMOUSLEVEL statement in FTP.DATA a parameter value greater than two. See the z/OS Communications Server: IP Configuration Reference for information about the ANONYMOUSLEVEL statement.

530: Closing control connection

Explanation

The client was attempting to log in to the FTP server as an anonymous user. The login was rejected after the root directory was changed for the anonymous login. It is now impossible to do a change directory to any other directory. The connection is severely limited and therefore the control connection is closed by the server.

System action

Login as an anonymous user is rejected. The control connection ends.

User response

The client program must issue an OPEN command to establish a new connection to the FTP server.

System programmer response

None.

530: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

530-: Current user *current user* remains logged in.

Explanation

The client was attempting to issue the FTP USER subcommand to change the login identity from *current user* to a new user login. The FTP server rejected the switch because FTP.DATA specifies ANONYMOUSLEVEL 3, which enables enhanced security checks.

System action

The USER command is rejected. The FTP client is still logged in as user *current user*. Control is returned to the client for further command processing.

User response

Issue the FTP CLOSE subcommand to end the session with the FTP server. Then issue the FTP OPEN subcommand to reinitialize the connection. Then log in as user *new user*.

System programmer response

None.

530-: email address rejected by user exit

Explanation

The FTP server is running with the user exit FTCHKPWD. The client was attempting to log in to the FTP server as an anonymous user and was prompted for an email address. The user exit does not allow the user to access the FTP server with the email address that was entered.

System action

FTP continues. The client login is rejected.

User response

Contact the owner of the FTP server to have the email address authorized in the FTCHKPWD user exit.

System programmer response

If necessary, update the FTCHKPWD user exit to authorize the email address.

530-: Error on *func* function call, errno=*errno*, rsncode=*errnojr*

Explanation

The client entered the USER and PASS commands to log in to the FTP server. While validating the user ID and password or password phrase of the client, a function issued by the FTP server failed.

func is the function call that failed.

errno is the z/OS UNIX System Services Return Code. These return codes are listed and described in the z/OS UNIX System Services Messages and Codes.

errnojr is the hexadecimal UNIX System Services Reason Code. The format of the 4-byte Reason Code is explained in the introduction to the Reason Code section of the z/OS UNIX System Services Messages and Codes, where the Reason Codes are listed.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer with the *func*, *errno* and *errnojr* values.

System programmer response

Correct the error indicated by *func*, *errno* and *errnojr*.

530-: error processing PASS command : *error*

Explanation

The client entered the USER and PASS commands to log in to the FTP server. The FTP server encountered an error attempting to setup the OMVS environment for the requested user ID.

error is the error message returned by the C run-time library.

System action

The login to the FTP server is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

Correct the error indicated by *error*. A previous 530 reply should contain further information in the reason code field.

530: Excessive bad passwords entered - USER command disabled

Explanation

The client attempted to log on to the FTP server system, but the user ID being used by the client had too many login attempts that were specified with an incorrect password or password phrase and this user ID was disabled.

System action

The user login is rejected. Control returns to the client for further command processing.

User response

The FTP session must end and reconnected to reset the number of bad password or password phrase attempts.

System programmer response

None.

530-: Initial filetype *file_type* is disabled for anonymous.

Explanation

The client was attempting to log into the FTP server as user ID anonymous. The FTP server rejected the login because FTP.DATA specified a FILETYPE value, *file_ type*, which was disabled for anonymous login users.

System action

Login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer of the server system.

System programmer response

If necessary, update FTP.DATA to contain consistent specifications for FILETYPE and ANONYMOUSFILETYPEJES, ANONYMOUSFILETYPESEQ, and ANONYMOUSFILETYPESQL.

530-: Internal processing error

Explanation

The client entered the PASS command. The __passwd function issued by the FTP server failed, indicating that an internal processing error occurred.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

There was a SAF/RACF error. A previous 530 reply should contain the reason code. This reason code contains the RACF return and reason codes, respectively.

530: Login attempt by *user ID* rejected by user exit

Explanation

The FTP server is running with the user exit FTCHKPWD. The user exit does not allow the user ID to access the FTP server.

System action

FTP continues. The client login is rejected.

User response

Contact the owner of the FTP server to have the user ID authorized in the FTCHKPWD user exit.

System programmer response

If necessary, update the FTCHKPWD user exit to allow the user ID to access the server.

530: Logon attempt by '*user_id*' rejected.

Explanation

The FTP server could not successfully validate the user's user ID and password or password phrase. The user login is rejected.

System action

The user login is rejected. FTP continues.

User response

This reply is preceded by a reply that indicates the reason for the failure. Correct the error indicated by the preceding reply. If necessary, contact the system programmer for the appropriate security authorization to access the FTP server.

System programmer response

If necessary, authorize the user to access the FTP server.

530: new password format invalid

Explanation

The PASS command was issued using the format old_password/new_password/new_password to change the password or password phrase of the user ID, but the second "/" could not be found in the password or password phrase entered with the PASS command.

System action

Login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Reissue the USER and PASS commands, using the correct format of the “old_password/new_password/new_password” on the PASS command.

System programmer response

None.

530: new passwords are not the same

Explanation

The PASS command was issued using the format old_password/new_password/new_password to change the password or password phrase of the user ID, but the second “new password” was not identical to the first “new password”. Both “new passwords” must be the same.

System action

Login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Reissue the USER and PASS commands, using the same password or password phrase for both occurrences of new_password.

System programmer response

None.

530: Not logged in.

Explanation

A command was issued to request a service from the FTP server, but the client was not currently logged in to a valid user ID for the server system. The command entered required the user to be logged in to a valid user ID.

System action

The command is rejected. Control returns to the client for further command processing.

User response

Log on to a valid user ID for the server system using the USER and PASS commands, then reissue the command. See the z/OS Communications Server: IP User's Guide and Commands for more information.

System programmer response

None. retrieve, store_data

530-: Number of groups exceeds the maximum number allowed

Explanation

The client entered the PASS command. The setgroups function issued by the FTP server failed, indicating that the number of supplementary groups for the specified user plus the basegid group exceeds the maximum number of groups allowed, or an invalid user is specified.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer to determine which supplementary groups your user ID is connected to.

System programmer response

Ensure that the user ID being used to log in to the FTP server is not connected to more than 300 supplementary groups.

530: PASS command failed

Explanation

The client entered the USER and PASS commands to log in to the FTP server. While validating the user ID and password or password phrase of the client, a function issued by the FTP server failed. See the previous 530 reply information for details.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

A previous 530 reply should contain further information in the reason code field.

530: PASS command failed - getpwnam() error : *error*

Explanation

The client entered the USER and PASS commands to log on to the FTP server. While validating the user ID and password or password phrase of the client, the getpwnam() function issued by the FTP server to obtain the OMVS information about the user ID failed.

error is the error message returned by the C run-time library for the getpwnam() function.

System action

The login to the FTP server is denied. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

Correct the error indicated by *error*. A previous 530 reply should contain further information in the reason code field.

530: PASS command failed - _passwd() error : *error*

Explanation

The client entered the USER and PASS commands to log on to the FTP server. While validating the user ID and password or password phrase of the client, the _passwd() function issued by the FTP server to obtain the OMVS information about the user ID failed.

error is the error message returned by the C run-time library for the _passwd() function.

System action

Login to the FTP server is denied.

User response

Contact the system programmer.

System programmer response

Correct the error shown in the reply code.

530-: Password was changed.

Explanation

The PASS command was entered in the format PASS **old_pass/new_pass/new_pass** to change the password or password phrase during login. The user password or password phrase was changed. The user can no longer log in to the system using the old password or password phrase.

System action

The user password or password phrase is changed. FTP continues.

User response

None.

System programmer response

None.

530-: Process does not have permission to set the UID

Explanation

The client entered the USER and PASS command. The setuid function issued by the FTP server failed, indicating that the process does not have appropriate privileges to set the UID.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

A previous 530 reply should contain further information in the reason code field.

530 : Server requires authentication

Explanation

The FTP server requires that a security environment is established before it can process a USER command.

System action

FTP continues.

User response

Issue the AUTH command to establish a security environment and then reissue the USER command.

System programmer response

None.

530 : Server requires authorized user

Explanation

The connection to the FTP server is protected by the GSSAPI security mechanism. The server FTP.DATA file contains the statement SECURE_LOGIN VERIFY_USER. The USER command that was received has a username that does not match the name found in the Kerberos credentials sent from the client during the authentication negotiation.

System action

The USER command is rejected. FTP continues.

User response

Log in using the username that matches the name that is passed in the Kerberos credentials.

System programmer response

If username match is not necessary, change the SECURE_LOGIN statement to have a value of either REQUIRED or OPTIONAL.

530-: StartDirectory *value* is disabled for anonymous.

Explanation

The client was attempting to log in to the FTP server as user ID anonymous. The FTP server rejected the login because FTP.DATA specified a STARTDIRECTORY of *value* that is in conflict with the ANONYMOUSFILEACCESS value.

System action

Login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer of the server system.

System programmer response

If necessary, update FTP.DATA to contain consistent specifications for STARTDIRECTORY and ANONYMOUSFILEACCESS.

530-: System authorization facility (SAF) had an error

Explanation

The client entered the PASS command. The setgroups function issued by the FTP server failed indicating the System authorization facility (SAF) had an error.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact your system programmer.

System programmer response

There was a SAF/RACF error. A previous 530 reply should contain the reason code. This reason code contains the RACF return and reason codes, respectively.

530-: The caller is not authorized

Explanation

The client entered the PASS command. The setgroups function issued by the FTP server failed, indicating that the caller is not authorized.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact your system programmer.

System programmer response

A previous 530 reply should contain further information in the reason code field.

530-: The email address entered is in an incorrect format.

Explanation

The client attempted to log in to the FTP server system as anonymous user. The server is setup to only allow valid email address to be entered as password or password phrase. The email address entered was not valid. This message will be followed by login failure reply.

System action

The user login is rejected. Control returns to the client for further command processing.

User response

The FTP session must end and reconnected to reset the number of bad password or password phrase attempts.

System programmer response

None.

530-: The newpass is not valid

Explanation

The client entered the PASS command. The __passwd function issued by the FTP server failed, indicating that the new password or password phrase is not valid, or does not meet the installation-exit requirements.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Use the correct format of **old_password/new_password/new_password** on the PASS command and reissue the USER and PASS commands.

System programmer response

None.

530-: The old password has expired

Explanation

The client entered the PASS command. The __passwd function issued by the FTP server failed, indicating that the password or password phrase expired.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Use the correct format of **old_password/new_password/new_password** on the PASS command and reissue the USER and PASS commands.

System programmer response

None.

530-: The old password is not authorized

Explanation

The PASS command was entered and the password or password phrase was not authorized.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Specify the correct password or password phrase and try the USER and PASS commands again.

System programmer response

None.

530-: The password is not authorized

Explanation

The FTP client sent the USER and PASS commands to the FTP server to log in. The password or password phrase specified on the PASS command was not authorized.

System action

The FTP server rejects the login to the user specified on the USER command. Control is returned to the client for further command processing.

User response

Login to the server again using the correct password or password phrase.

System programmer response

None.

530-: The process is currently not able to change UID

Explanation

The client entered the USER and PASS command. The setuid function issued by the FTP server failed , indicating that the process is currently not able to change UIDs.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

A previous 530 reply should contain further information in the reason code field.

530-: The username access was denied by SAF services

Explanation

The client entered the PASS command. The __passwd function issued by the FTP server failed, which indicates that the username access was denied by SAF services.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Reissue the USER and PASS commands with a valid user name and password or password phrase.

System programmer response

Use the *rsncode* value in the previous 530 reply to determine why the user ID access was denied. If your security product is IBM RACF, the *rsncode* contains the RACF return code and reason codes from the RACROUTE REQUEST=EXTRACT service. For a detailed description of the return and reason code values for the RACROUTE service, see the system macro information in z/OS Security Server RACROUTE Macro Reference for descriptions of the return and reason codes.

530-: The username is unknown

Explanation

The client entered the PASS command. The __passwd function issued by the FTP server failed, indicating that the user name specified is not defined to OMVS.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Reissue the USER and PASS commands with a valid user ID that is defined to OMVS, and a valid password or password phrase.

System programmer response

None.

530-: The username, oldpass or newpass argument is invalid

Explanation

The client entered the PASS command. The __passwd() function issued by the FTP server failed, indicating that one of the parameters is incorrect.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Reissue the USER and PASS commands with valid parameters.

System programmer response

None.

530-: The value of uid is incorrect

Explanation

The client entered the USER and PASS command. The setuid function issued by the FTP server failed, indicating that the UID is incorrect.

System action

The login to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

Verify that the UID in the OMVS segment associated with the user ID that is logging in is valid. A previous 530 reply should contain further information in the reason code field.

530: USER command failed

Explanation

The client entered a USER command to log in to the server. While validating the USER name, a function issued by the server failed.

System action

The login attempt to the user ID on the server system is rejected. Control is returned to the client for further command processing.

User response

Contact the system programmer.

System programmer response

A previous 530- reply should contain additional information in the reason code field.

530-: USER command failed. Switch from *current user* to *new user* not accepted.

Explanation

The client was attempting to issue the FTP USER subcommand to change the login identity from *current user* to *new user*. The FTP server rejected the switch because FTP.DATA specifies ANONYMOUSLEVEL 3, which enables enhanced security checks.

System action

The USER command is rejected. The FTP client is still logged in as user *current user*. Control is returned to the client for further command processing.

User response

Issue the FTP CLOSE subcommand to end the session with the FTP server. Then issue the FTP OPEN subcommand to reinitialize the connection. Then log in as user *new user*.

System programmer response

None.

530-: User *userid* is not allowed to access server's port.

Explanation

The user does not have access to the server port.

System action

The user login is rejected. FTP continues.

User response

Contact the system programmer.

System programmer response

If necessary, authorize the user to the FTP server port.

530: You must first login with USER and PASS.

Explanation

A command was issued to request a service from the FTP server, but the client was not currently logged in to a valid user ID for the server system. The command entered required the user to be logged in to a valid user ID.

System action

The command is rejected. Control returns to the client for further command processing.

User response

Log on to a valid user ID for the server system using the USER and PASS commands, then reissue the command. See the z/OS Communications Server: IP User's Guide and Commands for more information.

System programmer response

None.

531 reply codes

531 : Server requires client certificate for login processing

Explanation

The connection to the FTP server is protected by the TLS security mechanism. The server FTP.DATA file contains a SECURE_LOGIN statement with either the VERIFY_USER value or the REQUIRED value. When

these values are specified, the client must send a certificate to the server during the TLS authentication handshake. If the certificate is not sent, the FTP server rejects the USER command.

System action

FTP continues.

User response

Change the client configuration so that the client's certificate is sent to the FTP server as part of the TLS handshake. The z/OS FTP client does not require this option because it always sends its certificate. If this reply is received by a client that cannot send a certificate, the system programmer must change the FTP server before the client can log in.

System programmer response

If the client cannot send a certificate, consider changing the FTP server FTP.DATA file to specify SECURE_LOGIN OPTIONAL so that a client certificate is not required.

532 reply codes

532 : Username does not match name in client certificate

Explanation

The connection to the FTP server is protected by the TLS security mechanism. The server FTP.DATA file contains the statement SECURE_LOGIN VERIFY_USER. The USER command that was received has a username that does not match the name found in the certificate sent from the client during the authentication handshake.

System action

The USER command is rejected. FTP continues.

User response

Log in using the username that matches the name that is passed in the client certificate.

System programmer response

If username match is not necessary, change the SECURE_LOGIN statement to have a value of either REQUIRED or OPTIONAL.

533 reply codes

533 : All commands must be ENC protected

Explanation

The server received a command that was not protected at protection level private. The server is configured to only accept commands protected at protection level private.

System action

The command fails. FTP continues.

User response

Reissue the command using protection level private. If the client cannot send a protection level private command, the system programmer must change the FTP server before the client can log in.

System programmer response

If the client cannot send a protection level private command, consider changing the SECURE_CTRLCONN value in the server FTP.DATA file to allow other levels of protection.

533 : All commands must be protected

Explanation

The server received a command that was not protected but had not previously received a CCC command. A CCC command must be received on an authenticated connection before unprotected commands are allowed.

System action

The command fails. FTP continues.

User response

Either reissue the command as a protected command or issue a CCC command and reissue the unprotected command.

System programmer response

None.

534 reply codes

534 : CCC not supported

Explanation

The server FTP.DATA file contains the statement SECURE_CTRLCONN with a value of SAFE or PRIVATE. A CCC command was received but the control connection cannot be set to the clear protection level.

System action

The CCC command is rejected. FTP continues.

User response

None.

System programmer response

If a protection level of clear is desired for the control connection, change the SECURE_CTRLCONN statement to have a value of CLEAR.

534: Command *command* not allowed for connection to secure port

Explanation

The FTP client sent a command to the z/OS FTP server while the client was connected to the server's secure port, TLSPORT. The command is not allowed while you are logged in using the server's secure port.

In the reply text:

command
The command that the client sent to the server.

Example

```
Command:  ccc
>>>ccc
534 Command ccc not allowed for connection to secure port
```

System action

The command is ignored.

User response

Report the error to the system programmer.

System programmer response

If you need the command specified by the *command* value during a TLS-secured session, do not secure the session with the server's TLS-secured port. Instead, see the Customizing Transport Layer Security (TLS) and Kerberos security information in z/OS Communications Server: IP Configuration Guide for information about securing the FTP client and server for TLS security without resorting to the TLS-secured port. See the TLSPORT statement (FTP client and server) in z/OS Communications Server: IP Configuration Reference for more information about the secure port.

Problem determination

See the system programmer's response.

Source

z/OS Communications Server TCP/IP: FTP

534: Could not stop TLS security

Explanation

The FTP client sent an AUTH command, REIN command, or CCC command to the server while the session was secured with TLS. The server could not complete the command because an error occurred while the server was trying to stop TLS security for the control connection.

Example

```
Command: auth gssapi
    >>>AUTH GSSPI
    534 could not stop TLS security
```

System action

The FTP server closes the connection.

User response

Contact the system programmer.

System programmer response

Inspect the FTP server tracing and log messages in the SYSLOG to determine the cause of the error. If any FTP server tracing is active, the tracing that describes the error that the server encountered while stopping TLS is written to the SYSLOG. See the information about diagnosing FTP server problems with traces in z/OS Communications Server: IP Diagnosis Guide for information about FTP server tracing. The SYSLOG probably contains return code information from the gsk_secure_socket_shutdown() and gsk_secure_socket_close() calls. See the API reference information in z/OS Cryptographic Services System SSL Programming for more information about return codes from these function calls.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

534 : Server does not support the ADAT command for TLS secured connection

Explanation

The FTP server does not support the ADAT command for TLS secured connection.

System action

FTP continues.

User response

None.

System programmer response

None.

534 : Server does not turn off protection for TLS secured control connection

Explanation

The FTP server received a CCC command for a session that is protected by the TLS security mechanism. The control connection must have a protection level of private for a TLS secured session.

System action

The CCC command is rejected. FTP continues.

User response

None.

System programmer response

None.

534 : Server is not willing to accept security mechanism

Explanation

The server received an AUTH command specifying a security mechanism that the server is not configured to accept.

System action

The command fails. FTP continues.

User response

Reissue the command specifying an authentication mechanism that the FTP server is configured to accept or have the system programmer change the FTP server to accept the requested authentication mechanism.

System programmer response

Change the FTP server FTP.DATA file to specify EXTENSIONS AUTH_GSSAPI to accept the GSSAPI authentication mechanism or EXTENSIONS AUTH_TLS to accept the TLS authentication mechanism.

534: Server is not willing to accept security mechanism on this connection

Explanation

The server received an AUTH command specifying a security mechanism that the server does not support for the protocol used by the control connection. For example, AUTH GSSAPI is not supported when the control connection protocol is IPv6.

System action

The command fails. FTP continues.

User response

Reissue the command specifying an authentication mechanism that the FTP server is configured to accept, or start a new FTP session with the server using a protocol the server supports for the authentication mechanism you requested. For example, if the server rejected an AUTH GSSAPI command on an IPv6 connection, log in to that server using an IPv4 connection.

System programmer response

If the server rejected an AUTH GSSAPI command because the connection was IPv6, instruct the user to log in specifying the server's IPv4 address. If the server has no IPv4 address, code EXTENSIONS AUTH_TLS in the server's FTP.DATA to accept the TLS authentication mechanism. See the z/OS Communications Server: IP Configuration Reference for information about the EXTENSIONS statement.

534 : Server is protected and is not willing to accept another AUTH command

Explanation

The FTP server indicates that the session is already protected by a security mechanism and will not accept another AUTH command.

System action

FTP continues.

User response

If you want to change security mechanism, close the connection, reconnect to the FTP server, and issue the AUTH command with the new mechanism.

System programmer response

None.

534 : Server requires authentication before command processing

Explanation

The FTP server requires that a security environment is established before it can process the command.

System action

FTP continues.

User response

Issue the AUTH command to establish a security environment and then reissue the command.

System programmer response

None.

534 : Server requires authentication before PASS command

Explanation

The FTP server requires that a security environment is established before it can process a PASS command.

System action

FTP continues.

User response

Issue the AUTH command to establish a security environment and then reissue the PASS command.

System programmer response

None.

534 : Server requires authentication before USER command

Explanation

The FTP server requires that a security environment is established before it can process a USER command.

System action

FTP continues.

User response

Issue the AUTH command to establish a security environment and then reissue the USER command.

System programmer response

None.

534 : Server setup for TLS failed

Explanation

The FTP server attempted to set up a connection that is secured by the TLS security mechanism. The setup failed.

System action

FTP continues.

User response

Activate the FTP client and server traces as follows:

```
SITE DEBUG=(NONE,ACC,SOC(2))
DEBUG NONE ACC SOC(2)
```

Try the command again and contact the system programmer with the error message.

If you are not allowed to issue the SITE command to change the server trace options, ask the system programmer to set the options, close the session to the server, enter FTP again and try the failing subcommand

System programmer response

Use the FTP client and server traces to determine the cause of the error and correct the problem.

534: TLS negotiation failed -- data connection closed

Explanation

The FTP client and server failed during the negotiation step (also known as the handshake) to protect a data connection with the TLS mechanism.

System action

The command that was being processed failed. FTP continues.

User response

Activate the FTP client and server traces as follows:

```
SITE DEBUG=(NONE,ACC,SOC(2))
DEBUG NONE ACC SOC(2)
```

Try the command again and contact the system programmer with the error message.

If you are not allowed to issue the SITE command to change the server trace options, ask the system programmer to set the options, close the session to the server, enter FTP again and try the failing subcommand.

System programmer response

Use the FTP client and server traces to determine the cause of the error and correct the problem.

535 reply codes

535: Attempt to decrypt data failed

Explanation

The server call to the gss_unwrap() function failed. This reply is preceded by replies specifying the return codes returned from the failing function call. See those replies for further diagnosis.

System action

FTP continues.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the gss_unwrap() function.

535: Attempt to encrypt data failed

Explanation

The server call to the gss_wrap() function failed. This reply is preceded by replies specifying the return codes returned from the failing function call. See those replies for further diagnosis.

System action

FTP continues.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the gss_wrap() function.

535-: GSSAPI error major status code: *value* - *text*

Explanation

This reply displays the status code returned from a GSSAPI function call. This message is followed by a reply indicating the failing GSSAPI function call.

value is the hexadecimal value of the major status code.

text is the text describing the status code obtained by calling the gss_display_status() function.

System action

FTP continues.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the major status code.

535-: GSSAPI error minor status code: *value* - *text*

Explanation

This reply displays the status code returned from a GSSAPI function call. This message is followed by a reply indicating the failing GSSAPI function call.

value is the hexadecimal value of the minor status code.

text is the text describing the status code obtained by calling the gss_display_status() function.

System action

FTP continues.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the minor status code.

535 : Length *length* of received buffer is greater than PBSZ *size*

Explanation

The server received an encrypted message whose length was greater than the negotiated protection buffer size.

length is the length of the received encrypted message.

size is the maximum length of an encrypted message as negotiated with the client.

System action

FTP continues. The message is discarded.

User response

None.

System programmer response

None.

535 : Request to accept security context failed

Explanation

The server call to the gss_accept_sec_context() function failed. This reply is preceded by replies specifying the return codes returned from the failing function call. See those replies for further diagnosis.

System action

FTP continues. Authentication negotiation fails.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the gss_accept_sec_context() function.

535 : Request to acquire security credentials failed

Explanation

The server call to the gss_acquire_cred() function failed. This reply is preceded by replies specifying the return codes returned from the failing function call. See those replies for further diagnosis.

System action

FTP continues. Authentication negotiation fails.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the gss_acquire_cred() function.

535 : Request to import name failed

Explanation

The server call to the gss_import_name() function failed. This reply is preceded by replies specifying the return codes returned from the failing function call. See those replies for further diagnosis.

System action

FTP continues. Authentication negotiation fails.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the gss_import_name() function.

535 : Request to import the security context failed

Explanation

The server call to the gss_import_sec_context() function failed. This reply is preceded by replies specifying the return codes returned from the failing function call. See those replies for further diagnosis.

System action

FTP ends.

User response

None.

System programmer response

See the z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the gss_import_sec_context() function.

535: Request to load the Kerberos DLL library failed

Explanation

The connection to the FTP server is protected by the GSSAPI security mechanism. This requires the Kerberos DLL library to be loaded and the load of that library failed.

System action

The command fails and the connection to the FTP server is not established. FTP continues.

User response

Contact the system programmer.

System programmer response

Verify that these Kerberos libraries are added to the system data set concatenations:

EUVF.SEUVFLNK
Add to the LNKLSTxx PARMLIB member.

EUVF.SEUVFLPA
Add to the LPALSTxx PARMLIB member.

Module

EZAFTPRX

Destination

initRexec

536 reply codes

536 : Data connection protection *level* not supported

Explanation

The PROT command requested a data protection level that is not supported. The request to set the level is rejected.

level is one of the following ones:

- clear
- private
- safe
- confidential

The support by the FTP server for these levels is determined by the value specified on the SECURE_DATACONN statement in the FTP.DATA file for the server. SECURE_DATACONN specifies the minimum level of security allowed for the data connection.

PROT C is rejected if SECURE_DATACONN has a value of SAFE or PRIVATE.

PROT S is rejected if SECURE_DATACONN has a value of PRIVATE or NEVER. Also, it is rejected if the security mechanism is TLS.

PROT P is rejected if SECURE_DATACONN has a value of NEVER.

PROT E is always rejected.

System action

FTP continues.

User response

None.

System programmer response

None.

550 reply codes

550: Allocation for remote destination failed.

Explanation

The server attempted to allocate to a SYSOUT data set for the purpose to sending a data set to a remote destination (see SITE DEST). The allocation was unsuccessful.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

Examine the trace and look for trace messages with the tag *seq_alloc_dest*. These trace messages provide the reason codes for the dynamic allocation error.

550: Allocation of *dsname* failed while executing *command* command.

Explanation

The server attempted to allocate to a data set on a DASD volume. The dynamic allocation was unsuccessful.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

Examine the trace and look for trace messages with the tag *alloc_dasd*. These trace messages provide the reason codes for the dynamic allocation error.

550: Allocation of *dsname* failed while executing *cmd* command.

Explanation

The server attempted to allocate to a new data set to store data. The dynamic allocation was unsuccessful. *cmd* is STOR, STOU, or APPE.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

Examine the trace and look for trace messages with the tag *seq_create_file*. These trace messages provide the reason codes for the dynamic allocation error.

550: Allocation of *data_set* failed: (rc=*rc*, err=*err*, info=*info*)

Explanation

During load module transfer processing, the FTP server attempted to allocate the load library *data_set* using *dynalloc* and failed.

data_set
The name of the load library that the FTP server attempted to allocate

rc
The decimal return code of the allocation attempt.

err
The hexadecimal error code of the allocation attempt.

info
The hexadecimal information code of the allocation attempt.

System action

Load module processing ends. No files will be transferred. FTP waits for the next command from the FTP client.

User response

See z/OS MVS Programming: Authorized Assembler Services Guide for explanations for the *rc*, *err*, and *info* codes and take appropriate corrective action.

System programmer response

See z/OS MVS Programming: Authorized Assembler Services Guide for explanations for the *rc*, *err*, and *info* codes and take appropriate corrective action.

550: Allocation of temporary data set failed: (rc=*rc*, err=*err*, info=*info*)

Explanation

During load module transfer processing, the FTP server attempted to allocate a temporary data set using *dynalloc* and failed.

rc
The decimal return code of the allocation attempt.

err
The hexadecimal error code of the allocation attempt.

info
The hexadecimal information code of the allocation attempt.

System action

Load module processing ends. No files will be transferred. FTP waits for the next command from the FTP client.

User response

See z/OS MVS Programming: Authorized Assembler Services Guide, *dynalloc*, for explanations for the *rc*, *err*, and *info* codes and take appropriate corrective action.

System programmer response

See z/OS MVS Programming: Authorized Assembler Services Guide, *dynalloc*, for explanations for the *rc*, *err*, and *info* codes and take appropriate corrective action.

550-: anonymous login rejected by FTP server

Explanation

An FTP client attempted to log in as anonymous. The FTP server rejected the anonymous login.

System action

The client's session is ended.

User response

Log in to FTP as a different user. If you are authorized only as user anonymous, contact the system programmer with the error message.

System programmer response

Error messages related to anonymous login are written to syslogd if ftp server traces are enabled. If syslogd is not active, the error messages will be written to the operator console. Verify FTP is configured correctly to accept anonymous logins.

550 : command *command* fails: *message_prefix reason* (errno2 = *errno2*)

Explanation

The FTP server received the command command. While processing the command, a failure occurred in a Language Environment® (LE) library routine.

In the message text:

command
The command that the FTP server received.

message_prefix
The message identifier for reason. You can use the message prefix to find documentation for the *reason* value in z/OS Language Environment Runtime Messages.

reason
This is the reason reported by LE.

errno2
The errno2 value reported by LE. See z/OS Language Environment Runtime Messages for information about errno2 value reported by LE.

Example

```
Command:
quote xfif /tmp/trash/make my day
>>> xfif /tmp/trash/make my day
550 command XFIF fails: EDC5117I File exists. (errno2=0x05580075)
Command:
```

```
Command:
quote xfif /readOnly
>>> xfif /readOnly
550 command XFIF fails: EDC5141I Read-only file system. (errno2=0x05580076)
Command:
```

System action

The FTP server rejects the command.

User response

Report the error to the system programmer.

System programmer response

Use the *message_prefix* value to locate the reason specified the *reason* value in z/OS Language Environment Runtime Messages. If this does not identify the problem, see the problem determination. Correct the problem, and reissue the command.

Problem determination

Inspect the FTP server syslog trace for more information about the failure. Activate any FTP server trace option to capture trace information when FTP encounters an error from LE. If FTPLOGGING is active, messages EZYFS68I and EZYFS69I in the SYSLOG will include diagnostic information about the failure. Use the information in the SYSLOG trace to correct the problem.

See the following topics in z/OS Communications Server: IP Diagnosis Guide:

- Logging FTP server activity for information about FTPLOGGING.
- Diagnosing FTP server problems with traces for information about the FTP server SYSLOG trace.

Source

z/OS Communications Server TCP/IP: FTP

550: command *command* fails - unable to create named pipe *pathname*

Explanation

The server received an APPE (append) or STOR (store) command while UNIXFILETYPE=FIFO was configured. The FTP server attempted to create the named pipe while processing the command, but could not. See the UNIXFILETYPE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference for more information about the UNIXFILETYPE configuration option.

In the message text:

command
The command that the FTP server received.

pathname
The name of the named pipe.

Example

```
Command:
put /tmp/a /tmp/a/b/a
Binary tagged file translated with current data connection translation table
>>> PORT 9,2,1,3,4,49
200 Port request OK.
>>> STOR /tmp/a/b/a
```

```
550 command STOR fails - unable to create named pipe /tmp/a/b/a
Command:
```

System action

The command is rejected.

User response

Report the error to the system programmer.

System programmer response

Inspect the FTP server syslog trace for information about the failure. Activating any FTP server trace option is sufficient to capture trace information when FTP cannot create a named pipe. If FTPLOGGING is active, messages EZYFS68I and EZYFS69I in syslog will include diagnostic information. Use the information in the syslog trace to correct the problem.

See the following information in z/OS Communications Server: IP Diagnosis Guide:

- The information about FTPLOGGING.
- The information about FTP server SYSLOG trace.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

550: command *command* into *pathname* not supported when UNIXFILETYPE is FIFO

Explanation

The FTP server received a command that specified an existing file on the FTP server host while UNIXFILETYPE=FIFO was configured. The existing file is not a named pipe. The command must specify a named pipe when UNIXFILETYPE=FIFO is configured.

In the message text:

command
The command that the FTP server received.

pathname
The path name of the existing file on the FTP server host. See the UNIXFILETYPE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference for more information about the UNIXFILETYPE configuration option.

Example

```
Command:
put /etc/newhosts  /etc/hosts
Binary tagged file translated with current data connection translation table
>>> PORT 9,2,1,3,4,47
200 Port request OK.
>>> STOR /etc/hosts
550 command STOR into /etc/hosts not supported when UNIXFILETYPE is FIFO
Command:
```

System action

The command is rejected.

User response

Do one of the following actions:

- Specify a named pipe as the path name and reissue the file transfer.
- Change the UNIXFILETYPE configured value by sending a SITE command with the UNIXFILETYPE=FILE parameter to the FTP server, and reissue the file transfer. If your client is z/OS FTP, use the SIte subcommand. For other clients, use the QUOTE subcommand to send a SITE command to the server. See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information.

System programmer response

None.

Problem determination

None.

Source

z/OS Communications Server TCP/IP: FTP

550: Cannot create unique data set name for store unique of *dsname*.

Explanation

A unique name cannot be created to store a data set using the store unique command. The server appends numbers 1 to 999 to the end of the data set name to create a new name. This set of names is exhausted.

System action

The command is rejected. FTP continues.

User response

Change the file name to allow the server a set of names to search for uniqueness.

System programmer response

None.

550: Cannot create unique file name for store unique of *filename*.

Explanation

A unique name cannot be created to store a file in the hierarchical file system using the store unique command. The server appends numbers 1 to 999 to the end of the file name to create a new name. This set of names is exhausted.

System action

The command is rejected. FTP continues.

User response

Change the file name to allow the server a set of names to search for uniqueness.

System programmer response

None.

550: Cannot create unique member name for append to *dsname*

Explanation

An append was requested and the data set is a member of a partitioned data set (PDS). Before the append can occur, the member must be copied forward in the PDS and in the process is temporarily given a unique name. This process was attempted 999 times and a unique name was not found.

System action

The append is not performed.

User response

The unique names that are used for the copy are created by appending 1, then 2, and so forth to the end of member name (called the base name). If there are members of the PDS that have the same base name as the one for the append and the members are no longer needed, delete them and reissue the append request.

System programmer response

None.

550: Cannot create unique member name for store unique of *dsname*

Explanation

A unique name cannot be created to store a member of a partitioned data set (PDS) using the store unique command. The server appends numbers 1 to 999 to the end of the member name to create a new name. This set of names is exhausted.

System action

The command is rejected. FTP continues.

User response

Change the member name to allow the server a set of names to search for uniqueness.

System programmer response

None.

550: cannot determine characteristics of *pathname*

Explanation

The server received an XDSI command with *pathname* as a pathname parameter. The server could not obtain information about the path name needed to process the command.

pathname is the command parameter.

System action

The command is rejected.

User response

Contact the system programmer with the error.

System programmer response

Activate FTP server tracing with the FSC(3) option. Inspect the server FTP trace for information about why the characteristics of *pathname* could not be determined.

550: Cannot rename from partitioned data set *dsname* to a different partitioned data set *dsname*.

Explanation

You have attempted to rename a member of a partitioned data set (PDS). The new name is a member of a different PDS. A member of a PDS can be renamed only to a new member name within the same PDS.

System action

The rename is not performed.

User response

Provide a new name that is a name in the same PDS.

System programmer response

None.

550: closing control connection

Explanation

An error occurred while the client was logged in to FTP, or while the client was attempting to log in to FTP.

System action

The client's FTP session ends. FTP continues.

User response

Contact the system programmer with the error message.

System programmer response

Error messages related to the user's FTP session are written to syslogd if ftp server traces are enabled. If syslogd is not active, the error messages will be written to the operator console. Correct any errors found, and instruct the user to log in to FTP again.

550: *cmd* cmd failed : *error*

Explanation

The FTP client issued the command *cmd*. While processing the command, the FTP server issued a C run-time library function that did not complete successfully. *error* is the error message returned by the C run-time library.

System action

The command *cmd* is not executed.

User response

Reissue the command. If the problem persists, contact the system programmer with the error message.

System programmer response

Correct the error indicated by *error*.

550: *cmd* cmd failed. No files found.

Explanation

The LIST or NLST command issued for a z/OS UNIX directory failed because the directory did not contain any files.

System action

FTP continues processing with the next command

User response

None.

System programmer response

None.

550: *cmd* command failed - popen error: *error*

Explanation

The client issued the LIST or NLST command to list files in a z/OS UNIX directory. While processing the *cmd* command, the server issued the C run-time library routine popen(), which did not complete successfully. *error* is the error message returned by the C run-time library.

System action

The *cmd* command is rejected. The server waits for the next command to be entered by the client.

User response

Reissue the command. If the problem persists, contact the system programmer.

System programmer response

Correct the problem indicated by *error*.

550: *cmd* failed. Unknown HOME directory

Explanation

A command was issued that required the server to resolve the user's HOME directory name (for example, a path name was entered that began with the directory notation ~/) but the server was unable to determine the user's HOME directory.

System action

The command is rejected. FTP continues.

User response

Verify that the OMVS user ID has a HOME directory. If necessary, define a HOME directory for the user ID.

System programmer response

None.

550: *cmd* fails: *dsname*. User not authorized.

Explanation

A command was issued to store a data set. (*cmd* is STOR, STOU, or APPE.) The requested data set is protected by a security system such as RACF, and the user is not authorized to write to the data set.

System action

The data set is not stored. FTP continues.

User response

Contact the owner of the data set for authorization to store into the data set.

System programmer response

None.

550: *cmd* fails: *filename* is a directory and is not empty.

Explanation

The file that is named is a directory. The delete and rename subcommands support a directory name but the directory must be empty.

System action

The command is rejected. FTP continues.

User response

Reissue the command specifying an empty directory.

System programmer response

None.

550: *cmd* fails: *pathname* is a directory.

Explanation

An attempt was made to rename a z/OS UNIX file to a name that is an existing directory.

System action

FTP continues.

User response

None.

System programmer response

None.

550: *cmd* fails: *pathname* is not a directory.

Explanation

An attempt was made to rename a z/OS UNIX directory to a name that is an existing regular file.

System action

FTP continues.

User response

None.

System programmer response

None.

550: Command *command* fails: access to resource is denied by server.

Explanation

One of the following situations occurred:

- The FTP server received a command from an anonymous user. The command arguments specify an MVS or z/OS UNIX resource, such as a z/OS UNIX directory or MVS partitioned data set. Whichever file system the resource belongs to, the FTP server is configured to reject anonymous user access to that file system.
- The FTP server received a command from an anonymous user. The command arguments specify a z/OS UNIX named pipe. Anonymous users are not allowed to access named pipes.
- The FTP user tried to access a z/OS UNIX file system while the SAF SERVAUTH class was active, and that user was not permitted access to the resource profile EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.HFS. If the resource profile EZB.FTP.*sysname.ftpdaemonname*.ACCESS.HFS is defined in class SERVAUTH, FTP users must have

read access to that profile to be able to access the z/OS UNIX file system through the FTP server. Check for errors in the security product indicating that the user does not have read access to this resource.

In the message text:

command
The command that failed.

Example

```
Command:
user anonymous
>>> USER anonymous
331 Send password please.
PASSWORD:

>>> PASS
230 'ANONYMOUS' logged on.  Working directory is "USER2.".
Command:
put /etc/hosts /tmp/named.pipe
>>> PORT 9,2,1,3,4,10
200 Port request OK.
>>> STOR /tmp/named.pipe
550 Command STOR fails: access to resource is denied by server.
Command:
```

System action

The *command* command is rejected. The FTP server waits for the next command.

User response

Report the error to the system programmer.

System programmer response

If the user logged in anonymously,

- Inspect the default or explicitly coded value of ANONYMOUSFILEACCESS in the server's FTP.DATA. See z/OS Communications Server: IP Configuration Reference for information about ANONYMOUSFILEACCESS values. Change ANONYMOUSFILEACCESS to a value appropriate for your site. Stop the FTP server, then start it again, to enable the new ANONYMOUSFILEACCESS value.
- Determine whether the command arguments specified a named pipe. If you decide that the user should have access to the named pipe, direct the user to log in as a known user. Anonymous users are never allowed access to named pipes.

Check for errors in the security product indicating that the user does not have read access to the resource profile EZB.FTP.*sysname.ftpdaemonname*.ACCESS.HFS. If you want the user to have access to any z/OS UNIX file system, grant the user read access to that profile.

Rule: To access the z/OS UNIX file system, the user must log in again after access to the profile has been granted, and after the SERVAUTH class has been refreshed.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

550: Command *cmd* failed - pipe error: *error*

Explanation

The client issued the LIST or NLST command to list files in a z/OS UNIX directory. While processing the *cmd* command, the server issued the C run-time library routine pipe(), which did not complete successfully. *error* is the error message returned by the C run-time library.

System action

The *cmd* command is rejected. The server waits for the next command to be entered by the client.

User response

Reissue the command. If the problem persists, contact the system programmer.

System programmer response

Correct the problem indicated by *error*.

550: command *cmd* fails: *filename* does not exist

Explanation

The server recieved a command *cmd* with *filename* as a parameter. *filename* does not exist.

System action

The command is rejected. FTP continues.

User response

Reissue the command specifying a file or data set that exists.

System programmer response

None.

550: Command *cmd* fails: *filename* is a character special file.

Explanation

The file that is named is a character special file. The file transfer, delete, and rename subcommands do not support files of this type.

System action

The command is rejected. FTP continues.

User response

Reissue the command specifying a name of a file that is not a character special file.

System programmer response

None.

550: Command *cmd* fails: *filename* is an unknown type.

Explanation

The file that is named is an unknown type. The file transfer, delete, and rename subcommands do not support files of this type.

System action

The command is rejected. FTP continues.

User response

Reissue the command specifying a name of a file that is not an unknown file type.

System programmer response

None.

550: Command *cmd* fails: *filename* is a directory.

Explanation

The file that is named is a directory. The RETR, STOR, STOU, and APPE commands do not support file transfer for a directory file.

System action

The command is rejected. FTP continues.

User response

Reissue the command specifying a name of a file that is not a directory.

System programmer response

None.

550: Command *cmd* fails: *filename* is a pipe or FIFO.

Explanation

The FTP server received a command that specified an existing file on the FTP server host while UNIXFILETYPE=FILE was configured. The existing file is a z/OS UNIX named pipe or FIFO special file. The command must specify a z/OS UNIX regular file when UNIXFILETYPE=FILE is configured.

In the message text:

cmd
The command that the FTP server received.

filename
The path name of the named pipe or FIFO special file.

Example

```
Command:
put /etc/hosts /tmp/sample.fifo
>>> PORT 9,2,5,6,4,22
```

```
200 Port request OK.
>>> STOR /tmp/sample.fifo
550 Command STOR fails: /tmp/sample.fifo is a pipe or FIFO.
Command:
```

System action

The command is rejected. FTP continues.

User response

Do one of the following actions:

- Reissue the command with the name of a file that is not a pipe or FIFO special file specified.
- Change the UNIXFILETYPE configured value by sending a SITE command with the UNIXFILETYPE=FIFO parameter to the FTP server, and reissue the file transfer.
  - If your client is z/OS FTP, use the SIte subcommand.
  - For other clients, use the QUOTE subcommand to send a SITE command to the server.

  See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information.

System programmer response

None.

550: command *command* fails: filetype is *file type*

Explanation

The client issued the *command* command to the FTP server. The FTP server is operating in filetype mode *file type*; *command* is supported only in file type mode SEQ.

System action

The *command* command is rejected. The FTP server waits for the next command from the client.

User response

If possible, issue the SITE FILETYPE=SEQ subcommand to the FTP server to change to the FILETYPE SEQ operating mode, then reissue *command*.

System programmer response

None.

550: Command *cmd* fails - *name* is of an unsupported type

Explanation

The specified command was sent to the server, but the server does not support that command for the specified type of data set.

In the message text:

cmd
The command name that is specified on the FTP command.

name
The data set name that is specified on the FTP command.

Example

```
mvsget /etc/ftp.data 'user1.ftp.ps'
EZA1701I >>> xdss /etc/ftp.data
550 Command XDSS fails – /etc/ftp.data is of an unsupported type
```

System action

FTP continues processing.

Operator Response

No action is needed.

User Response

Reissue the subcommand with a data set of a supported type. For more information about the MVSGET or MVSPUT subcommand, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

No action is needed.

Problem Determination

Not applicable.

550: command *command* fails - *pathname* must be an MVS directory

Explanation

The FTP server received a command with a pathname parameter. The parameter must be an MVS directory (a PDS or PDSE). The path name exists, but it is not an MVS directory.

command is the command that specified the pathname parameter.

pathname is the pathname parameter

System action

The command is rejected. Control returns to the client for further command processing.

User response

Reissue the command, specifying an MVS directory as *pathname*.

System programmer response

None.

550 : command *command* fails: *pathname* - user is not authorized

Explanation

The FTP server received a command that specifies a path name as its target. Part of the path name is protected by a security system, such as RACF. The user did not have sufficient authority to create or access the specified path name.

In the message text:

command
The command that the FTP server received.

pathname
The path name that could not be created or accessed.

Example

```
Command:
mkfifo f /u/user1/fifo
>>> xfif /u/user1/fifo
550 command XFIF fails: /u/user1/fifo - user is not authorized.
Command:

Command:
quote xfif /tmp/my_fifo
>>> xfif /tmp/my_fifo
550 command XFIF fails: /tmp/my_fifo - user is not authorized
Command:

Command:
put /etc/hosts /u/user1/named.pipe
>>> PORT 9,2,1,3,4,28
200 Port request OK.
>>> STOR /u/user1/named.pipe
550 command STOR fails: /u/user1/named.pipe - user is not authorized
Command:
```

System action

The FTP server rejects the specified command.

User response

Contact the security administrator to obtain the necessary authorization to create or access the path name.

System programmer response

None.

Problem determination

Not applicable.

Source

z/OS Communications Server TCP/IP: FTP

550: command *command* is not available for *pathname*

Explanation

The client issued the *command* command to the FTP server. The FTP server was not able to execute the command for *pathname*, for one of the following reasons.

The file was not a z/OS UNIX file. *command* is supported only for z/OS UNIX files.
An I/O error occurred while the FTP server was reading from the file system.
For FILETYPE=JES, a pathname must be in the form of JOBxxxxx, TSUxxxxx, APCxxxxx, or TSUxxxxx.

If *command* is SIZE, additional reasons might cause the command to be rejected:

The file size is too large to be represented by a C int type variable (two words of storage). *Command* is not supported for files of sizes larger than can be represented as an int type variable.
The file is a z/OS UNIX file, but it is not a regular z/OS UNIX file as defined by UNIX System Services. SIZE is supported for regular z/OS UNIX files only.

System action

The *command* command is rejected. The FTP server waits for the next command from the client.

User response

Verify *pathname* was entered correctly, and that *pathname* represents a z/OS UNIX file of a supported size and type, as applicable. Correct any errors, then issue *command* again. If the problem recurs, report it to the system programmer.

System programmer response

Error messages related to *pathname* retrieval are written to syslogd if ftp server traces are enabled. If syslogd is not active, the error messages will be written to the operator console. Correct any errors, then have the user issue *command* again.

550: command *command* is not supported for mode *mode*

Explanation

The FTP client issued command *command* to the FTP server. The FTP server's data transfer mode is *mode*. Command *command* is not supported for data transfer mode *mode*.

System action

The command is rejected. FTP waits for the next command from the FTP client.

User response

If possible, issue the FTP **mode** subcommand to set the data transfer mode to a value valid for *command*. Then issue *command* again. Please see z/OS Communications Server: IP User's Guide and Commands for information on valid data transfer modes for *command*.

System programmer response

None.

550: command *command* is not supported for structure *structure*

Explanation

The FTP client issued command *command* to the FTP server. The FTP server's file structure is *structure*. Command *command* is not supported for file structure *structure*.

System action

The command is rejected. FTP waits for the next command from the FTP client.

User response

If possible, issue the FTP STRUCTURE subcommand to set the file structure to a value valid for *command*. Then issue *command* again. Please see z/OS Communications Server: IP User's Guide and Commands for information on valid file structures for *command*.

System programmer response

None.

550: command *command* is not supported for type *type*

Explanation

The FTP client issued command *command* to the FTP server. The FTP server's data transfer type is set to *type*. Command *command* is not supported for data transfer type *type*.

System action

The command is rejected. FTP waits for the next command from the FTP client.

User response

If possible, issue the FTP TYPE subcommand to set the data transfer type to a value valid for *command*. Then issue *command* again. Please see z/OS Communications Server: IP User's Guide and Commands for information on valid data transfer types for *command*.

System programmer response

None.

550-: command *command* rejected - file transferred while SBSENDEOL not CRLF

Explanation

Your FTP client sent the command *command* to the server as part of a stream mode restart of a Type ASCII file retrieve. Earlier during this login session, you transferred a file while these configuration options were set: Encoding was SBCS, Mode was stream, Type was ASCII, and SBSENDEOL was a value other than CRLF. Stream mode restart of file transfer is not reliable under these conditions. Unpredictable results will occur if you restart such a file transfer.

command is the command the FTP client sent to the FTP server.

See z/OS Communications Server: IP Configuration Reference for more information about configuration options such as SBSENDEOL, ENCODING, MODE, and TYPE. See the SIte subcommand in z/OS

Communications Server: IP User's Guide and Commands for more information about the SBSENDEOL parameter.

System action

The FTP server waits for the next command.

User response

Do not attempt to restart this file transfer. Instead, retrieve the file again in its entirety.

System programmer response

The SBSENDEOL value, CRLF, is the EOL sequence defined for FTP by RFC 959. It is the appropriate value to use for most file transfers. Do not configure an SBSENDEOL value other than CRLF unless you are certain your FTP client supports it for inbound file transfer. When only certain clients that log in to this server require an alternate SBSENDEOL value, do the following actions:

- Configure SBSENDEOL in the server's FTP.DATA to be CRLF by default.
- Use a SITE command with the SBSENDEOL parameter to change the SBSENDEOL value only when the FTP client supports the alternate value. For z/OS FTP clients, the SIte subcommand is available to send a SITE command to the FTP server.

550: *command* fails: *dsname*. User not authorized

Explanation

The *command* command was issued to read a data set. The requested data set is protected by a security system such as RACF, and the user is not authorized to read the data set.

System action

The data set is not sent. FTP continues.

User response

Contact the owner of the data set for authorization to read the data set.

System programmer response

None.

550: *command* fails: *pathname*. User not authorized

Explanation

The LIST or NLST command was issued to list members of a partitioned data set, but the requested data set was protected by a security system such as RACF, and the user was not authorized to read the data set.

System action

The LIST or NLST command is rejected.

User response

Contact the owner of the data set for authorization to read the data set.

System programmer response

None.

550: command SIZE is not supported for the current data connection translate table when type is *type*

Explanation

The server received a SIZE command. SIZE is not supported for the translate table in use on the data connection in combination with the current data transfer type.

type is the current data transfer type.

System action

FTP continues.

User response

None.

System programmer response

None.

550: command SIZE rejected - *pathname* contains CR characters

Explanation

The client sent a SIZE pathname command to the FTP server while the data transfer type setting was ASCII. The file pathname contains carriage return (CR) characters. The FTP server cannot complete the SIZE command for any file containing CR characters when the data transfer type is ASCII.

pathname is the name of a z/OS UNIX file that is the target of the SIZE command.

System action

The FTP server stops processing the SIZE command and waits for another command from the client.

User response

If you are using the SIZE command to learn the byte transfer size for a certain file whenever the data transfer type is ASCII, no further action is possible. If you do not require the data transfer type to be ASCII, change the data transfer type from ASCII. See the documentation for your FTP client to learn how to change the data transfer type.

System programmer response

None.

550: command SIZE rejected - *pathname* is not an z/OS UNIX file

Explanation

The server received a SIZE command from the client. The target of the SIZE command is not a z/OS UNIX file. The FTP server supports SIZE only for z/OS UNIX files.

pathname is the target of the SIZE command.

System action

Processing continues.

User response

None.

System programmer response

None.

550: Command terminated due to CPU time limit exceeded

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS kill -s SIGXCPU command or the CPU time limit exceeded.

System action

The command in progress and the FTP server session process end.

User response

Contact the system programmer.

System programmer response

If the server process was stopped due to CPU time limit exceeded, check the MAXCPUTIME parameter in BPXPRMxx.

550: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

550: could not delete *dataset*

Explanation

While the FTP server was processing a DELE (delete) command from the FTP client, the server encountered an error and could not complete the request. This reply can appear by itself, or as part of a group of messages.

In the message text:

dataset
The MVS data set specified by the DELE command.

Example

```
delete etchost
>>>DELE etchost
550-System completion code and reason: 213-24
550 could not delete USER5.PDS(ETCHOST)
Command:
```

System action

The FTP server stops processing the DELE command.

Operator response

None.

User response

If this reply is part of a group of replies, inspect the earlier replies for information about the reason the delete failed; otherwise, report the error to the system programmer.

System programmer response

If this reply appears by itself, inspect the FTP server syslog trace output for diagnostic messages related to the MVS data set specified by the *dataset* value. Correct the problem, and ask the user to delete the specified dataset. If this reply is part of a group of replies, follow the steps recommended for the earlier replies to correct the problem.

Problem determination

For information about enabling and capturing the FTP server sylog trace, see the information about diagnosing FTP server problems with traces in z/OS Communications Server: IP Diagnosis Guide.

Source

z/OS Communications Server TCP/IP: FTP

550: Data set *dsname* is migrated and NoAutoRecall is specified.

Explanation

A command was issued to process a data set, but the data set is migrated and the FTP server is currently in NoAutoRecall mode.

System action

The command is rejected.

User response

Issue the "SITE AUTORECALL" command to allow the data set to be recalled, and then reissue the FTP command.

System programmer response

None.

550: Data set *dsname* not found

Explanation

The server attempted to retrieve a data set (that is, a physical sequential data set or member of a partitioned data set). The data set was not found.

System action

The command is rejected. FTP continues.

User response

Ensure that the data set exists and that the fully qualified name used for the retrieve is correct.

System programmer response

None.

550: "*directory*" data set does not exist.

Explanation

The RMD was issued to delete the partitioned data set *directory*, but the server could not find the data set to delete it.

System action

The RMD command is rejected. Control returns to the client for further command processing.

User response

Verify that the correct data set name was entered. If necessary, reissue the command with the correct data set name.

System programmer response

None.

550: *dsname* is a partitioned data set and no member was specified on the *cmd* command.

Explanation

The server attempted to store to a partitioned data set (PDS) but did not provide a member name. *cmd* is STOR, STOU, or APPE.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

Provide a member name for the PDS.

550: *dsname* is a physical sequential data set and a member was specified on the command.

Explanation

You requested a member of a data set but the data set that was named is a physical sequential data set (PDS) and does not have members.

System action

The data set is not stored. FTP continues.

User response

Provide the correct name of the PDS that contains the member requested.

System programmer response

None.

550: *dsname* is not on a direct access volume. It may not be deleted.

Explanation

The data set to be deleted is not on a direct access volume.

System action

The data set is not deleted. FTP continues.

User response

Make sure that the data set name is for a data set that can be deleted. A tape data set is an example of data set that cannot be deleted.

System programmer response

None.

550: *dsname* is not on a direct access volume. It may not be renamed.

Explanation

The data set to be renamed is not on a direct access volume.

System action

The data set is not renamed. FTP continues.

User response

Make sure that the data set name is for a data set that can be renamed. A tape data set is an example of data set that cannot be renamed.

System programmer response

None.

550: *dsname* used exclusively by someone else.

Explanation

Either a data transfer (retrieve or store), a delete, or a rename of a member of a partitioned data set (PDS) was requested and the member requested is currently in use.

System action

The operation is not performed.

User response

Try the operation later when no one else is using the member of the PDS.

System programmer response

None.

550: DELE fails: *dsname* does not exist.

Explanation

The DELE command was issued to delete a data set. The delete was unsuccessful because the data set does not exist.

System action

None. FTP continues.

User response

Make sure that the correct data set name is entered and that the data set is catalogued.

System programmer response

None.

550: DELE fails: *dsname*. User not authorized.

Explanation

The DELE command was issued to delete a data set. The requested data set is protected by a security system such as RACF, and the user is not authorized to delete the data set.

System action

The data set is not deleted. FTP continues.

User response

Contact the owner of the data set for authorization to delete it.

System programmer response

None.

550: directory remains "*file_name*".

Explanation

A CWD command was received to change the current working directory, but the server was not able to successfully change the current working directory. This reply is preceded by other replies with additional information about the error.

System action

The working directory is not changed. FTP continues.

User response

Correct the errors indicated by the replies that preceded this one.

System programmer response

None.

550: DSORG=DA requires structure: FILE, mode: STREAM, and transfer type: IMAGE.

Explanation

A RETR command was issued but one or more of the following required conditions are not met: FILE structure, STREAM mode, and/or IMAGE transfer type.

System action

The command is rejected. FTP continues.

User response

If a retrieval of a DA file was intended, use the STAT FTP command to display the current settings for your FTP connection. Use the STRUC F, MODE S, and/or TYPE I commands as necessary to alter the settings for your connection.

System programmer response

None.

550: error allocating *new_directory*

Explanation

The MKD command was issued to create the new PDS *new_directory*, but the server was unable to allocate the PDS.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Contact the system programmer for the server system.

System programmer response

Determine why the PDS could not be allocated and correct the problem.

550: Error allocating storage for *type*

Explanation

The FTP server was not able to allocate the storage for the specified type necessary to process the LIST or NLST command.

System action

The LIST or NLST command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the FTP server system.

System programmer response

The FTP server might need to be started with a larger region size.

550: Error allocating tape data set *dsname*

Explanation

The server attempted to allocate to a data set on a tape volume. The dynamic allocation was unsuccessful.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

Examine the trace and look for trace messages with the tag *alloc_tape*. These trace messages provide the reason codes for the dynamic allocation error.

550: Error deleting migrated data set *dsname*

Explanation

The services of DFHSM were invoked to delete a data set that is migrated. DFHSM cannot delete the data set.

System action

The data set is not deleted. FTP continues.

User response

Recall the data set and try the command again.

System programmer response

None.

550-: error initializing FTP server

Explanation

An error occurred while a client was attempting to log in to FTP. FTP was not able to complete the login.

System action

The client's session is ended.

User response

Contact the system programmer with the error message.

System programmer response

Error messages related to the anonymous login are written to syslogd if FTP server traces are enabled. If syslogd is not active, the error messages will be written to the operator console. Correct any errors, and instruct the user to log in to FTP again.

550: Error mounting volume containing data set *dsname*

Explanation

The volume containing the requested data set *dsname* was not mounted to the FTP server system. The FTP server attempted to have the volume mounted, but did not succeed.

System action

The command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the FTP server system.

System programmer response

Determine why the requested volume cannot be mounted to the MVS system.

550: Error opening *data_set_name*

Explanation

The LIST or NLST command requested members of a PDS, but the FTP server was unable to open the PDS to read the directory. This can be a temporary problem, for example the data set is currently in use, or it can be a permanent error with the data set.

System action

The LIST or NLST command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Correct the problem with the data set.

550: error reading PDS directory

Explanation

The LIST or NLST command requested members of a partitioned data set, but the FTP server was unable to read the directory of the PDS.

System action

The LIST or NLST command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Correct the problem with the data set.

550: Error recalling data set *data_set*

Explanation

The LIST or NLST command requested members of a partitioned data set. The PDS was migrated and needed to be recalled to read the PDS directory. The FTP server attempted to recall the data set, but was unable to successfully recall the data set.

System action

The LIST or NLST command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Determine why the data set cannot be recalled and correct the problem.

550: Error recalling data set *data_set* (rc=*rc*)

Explanation

A RETR request was received for a data set. The data set was migrated and needed to be recalled. The FTP server attempted to recall the data set, but was unable to successfully recall the data set.

System action

The RETR command is rejected.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

Determine why the data set cannot be recalled and correct the problem.

550: File *filename* not found.

Explanation

The server attempted to retrieve an hierarchical file system (z/OS UNIX) file. The file was not found.

System action

The command is rejected. FTP continues.

User response

Ensure that the file exists and that you have access to all of the directories in the path to the file.

System programmer response

None.

550: *file_name* requests a nonexistent partitioned data set. Use MKD command to create it.

Explanation

The store request names a partitioned data set (PDS) that does not exist.

System action

The data set is not sent. FTP continues.

User response

Either name an exiting PDS or use MKD command to create a PDS into which the member will be stored.

System programmer response

None.

550-: GSSAPI error major status code: *value* - *text*

Explanation

This reply displays the status code returned from a GSSAPI function call. This message is followed by a reply indicating the failing GSSAPI function call.

value is the hexadecimal value of the major status code.

text is the text describing the status code obtained by calling the gss_display_status() function.

System action

FTP continues.

User response

None.

System programmer response

See z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the major status code.

550-: GSSAPI error minor status code: *value* - *text*

Explanation

This reply displays the status code returned from a GSSAPI function call. This message is followed by a reply indicating the failing GSSAPI function call.

value is the hexadecimal value of the minor status code.

text is the text describing the status code obtained by calling the gss_display_status() function.

System action

FTP continues.

User response

None.

System programmer response

See z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the minor status code.

550: Index *number* is greater than number of spool files for *jobid*

Explanation

User attempted to retrieve a specific spool file from JES using the FTP GET command. JES output files are numbered sequentially from one. The specified number is greater than the number of spool files for the job.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the FTP GET command with the correct job ID and index.

System programmer response

None.

550: internal error processing *command* command

Explanation

An internal error occurred while the FTP server was processing the specified command.

In the message text:

command
The command that the FTP server received.

Example

Not applicable.

System action

FTP rejects the command.

User response

Report the error to the system programmer.

System programmer response

Obtain the diagnostic materials identified in the information about documenting server problems in z/OS Communications Server: IP Diagnosis Guide. Contact the IBM Software Support Center.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

550-: Internal error processing *function* SSOBRETN=*rc*.

Explanation

The specified function was using the JES SubSystem Interface (SSI) and received the specified SSOBRETN return code value. The return codes are documented in z/OS MVS Using the Subsystem Interface .

System action

No data is sent. FTP continues.

User response

Ensure that the JES subsystem is active.

System programmer response

None.

550: Invalid cancel request

Explanation

A DELETE command was issued. The command was not formed correctly.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Invalid jobname/Jobid combination

Explanation

JES could not perform the requested function because the exact JOBNAME and JOBID combination specified in the command could not be located.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: JES cannot find output for *jobid*

Explanation

User attempted to retrieve data for a specific job ID. The job ID specified in the command was not found.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command.

System programmer response

None.

550: JES cannot find output for *jobid*, JesPutGet aborted

Explanation

User attempted to retrieve data for a specific job ID. The job ID specified in the command was not found.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command.

System programmer response

None.

550: JES internal reader allocation failed

Explanation

In preparation of submitting a job to MVS the Internal Reader needed to be allocated. The allocation of the Internal Reader failed.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: JES internal reader open failed

Explanation

In preparation of submitting a job to MVS the Internal Reader needed to be opened. The request to open the Internal Reader failed.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: JES is unable to provide spool data set name now

Explanation

User attempted to retrieve spool files from JES. Requested dataset is open.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Issue the command later

System programmer response

None.

550: JES is unable to provide spool data set name now, JesPutGet aborted

Explanation

User attempted to retrieve spool files from JES. Requested dataset is open.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Issue the command later

System programmer response

None.

550: JES spool file allocation failed for *dsname*

Explanation

An allocate of a spool file for get processing failed.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: JES spool file open failed for *dsname*

Explanation

While attempting to open a spool file for processing, an error occurred.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: JESPUT failed, could not allocate receive buffer

Explanation

A buffer was not available while attempting to retrieve a spool output.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: JesPutGet aborted

Explanation

See replies prior to this 550 reply.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: JesPutGet aborted, internal error

Explanation

A GET command was issued with a SITE FILETYPE=JES argument in effect. The GET command requested the output to be automatically retrieved. The output was not retrieved because of an internal processing error in FTP.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Attempt to retrieve the job from JES explicitly. If this problem prevails, contact your system support personnel for assistance.

System programmer response

Diagnose the problem.

550: JesPutGet aborted, job not found

Explanation

A GET command was issued with a SITE FILETYPE=JES argument in effect. The GET command requested the output to be automatically retrieved. The output was not available to be retrieved within the time period allowed for the JOB to complete execution.

System action

FTP server continues normal execution. The FTP client waits for the next command input. The job submitted might or might not complete in the near future.

User response

Explicitly retrieve the job from JES if and when the job completes execution.

System programmer response

None.

550: JesPutGet aborted, timeout exceeded

Explanation

A GET command was issued with a SITE FILETYPE=JES argument in effect. The GET command requested the output to be automatically retrieved. The output was not available to be retrieved within the time period allowed for the JOB to complete execution.

System action

FTP server continues normal execution. The FTP client waits for the next command input. The job submitted might or might not complete in the near future.

User response

Explicitly retrieve the job from JES if and when the job completes execution.

System programmer response

None.

550: JesPutGet terminated

Explanation

During the PUT or GET processing, a timer expired before the job completed.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Explicitly retrieve the job from JES.

System programmer response

None.

550: Job name not found

Explanation

JES could not locate the JOBNAME specified in the command.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Job not cancelled, duplicate jobnames and no Jobid

Explanation

JES could not perform the requested function because more than one JOBNAME exists on which JES could perform the action.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Job not cancelled, job on output queue

Explanation

A DELETE (JES cancel) command was issued against a job that was executing. The job completed execution and all output was found to be on the output queue.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Jobid *jobid* not found

Explanation

JES could not locate the job ID specified in the command.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Jobid *jobid* not found for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner*

Explanation

JES could not locate the job ID specified in the command given the filter settings for JESJOBNAME, JESSTATUS, and JESOWNER.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command. Possibly, use the SITE command to change the JESJOBNAME, JESSTATUS, or JESOWNER if it does not match those of the name, status or owner of the specified job ID. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Jobid with invalid syntax for subsystem

Explanation

The DELETE command issued did not conform to the required syntax.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Mismatched quotes on pathname *pathname*

Explanation

The pathname provided for a data transfer (retrieve or store), delete, or rename request was enclosed in a unbalanced set of single quotes.

System action

The request is not performed.

User response

Enclose the data set name in balanced quotes -- a quote at the beginning and the end of the name.

System programmer response

None.

550: MKD failed. Dcbdsn data set *dcbdsn_name* does not exist.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN was in effect specifying that all new data sets be created with the same characteristics as the data set *dcbdsn_name*. The server could not find the model data set *dcbdsn_name* to determine the data set characteristics.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Use the SITE command to either specify a different DCBDSN data set, or to specify the data set characteristics without using the DCBDSN model data set parameter. After changing the appropriate SITE parameters, reissue the MKD command.

System programmer response

None.

550: MKD failed. Dcbdsn data set *dcbdsn_name* is not on a direct access volume.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN was in effect specifying that all new data sets be created with the same characteristics as the data set *dcbdsn_name*. However, the model data set *dcbdsn_name* was not on a direct access volume and therefore could not be used as a model data set.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Use the SITE command to either specify a different DCBDSN data set, or to specify the data set characteristics without using the DCBDSN model data set parameter. After changing the appropriate SITE parameters, reissue the MKD command.

System programmer response

None.

550: MKD failed. Dcbdsn data set *dcbdsn_name* is a VSAM data set.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN was in effect specifying that all new data sets be created with the same characteristics as the data set *dcbdsn_name*. However, the model data set *dcbdsn_name* was a VSAM data set and therefore could not be used as a model for the data set characteristics.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Use the SITE command to either specify a different DCBDSN data set, or to specify the data set characteristics without using the DCBDSN model data set parameter. After changing the appropriate SITE parameters, reissue the MKD command.

System programmer response

None.

550: MKD failed. Dcbdsn data set *dcbdsn_name* has an invalid dsorg.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN was in effect specifying that all new data sets be created with the same characteristics as the data set *dcbdsn_name*. However, the model data set *dcbdsn_name* was neither a partitioned data set or a physical sequential data set, and therefore could not be used as a model for the data set characteristics.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Use the SITE command to either specify a different DCBDSN data set, or to specify the data set characteristics without using the DCBDSN model data set parameter. After changing the appropriate SITE parameters, reissue the MKD command.

System programmer response

None.

550: MKD failed. Dcbdsn data set *dcbdsn_name* has a recfm of *recfm* which is invalid for a PDS.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN was in effect specifying that all new data sets be created with the same characteristics as the data set *dcbdsn_name*. However, the model data set *dcbdsn_name* had a record format *recfm* that is not valid for a PDS. Record formats FBS, VBS, and VS are not valid record formats for a PDS.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Use the SITE command to either specify a different DCBDSN data set, or to specify the data set characteristics without using the DCBDSN model data set parameter, or a combination of DCBDSN and RECFM SITE parameters to use all of the characteristics of the model DCBDSN data set except the record format, which will be overridden by the RECFM parameter. After changing the appropriate SITE parameters, reissue the MKD command.

System programmer response

None.

550: MKD failed. Dcbdsn data set *dcbdsn_name* is migrated and noautorecall is specified.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN was in effect specifying that all new data sets be created with the same characteristics as the data set *dcbdsn_name*. However, the model data set *dcbdsn_name* was migrated and the server was currently in No AutoRecall mode, therefore the model data set could not be recalled to determine the data set characteristics.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Use the SITE AUTORECALL command to allow the DCBDSN data set to be recalled, then reissue the MKD command.

System programmer response

None.

550: MKD failed. Error locating dcbdsn data set *dcbdsn_name*.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN was in effect specifying that all new data sets be created with the same characteristics as the data set *dcbdsn_name*. However, an error occurred when the server issued the LOCATE macro to locate the model data set *dcbdsn_name*. The server was unable to determine the characteristics of the model data set *dcbdsn_name* and therefore could not allocate the new data set.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Use the SITE command to either specify a different DCBDSN data set, or to specify the data set characteristics without using the DCBDSN model data set parameter. After changing the appropriate SITE parameters, reissue the MKD command.

System programmer response

None.

550: MKD failed. Unit=*unit_name* invalid for PDS.

Explanation

The MKD command was issued to create a new PDS, but the current setting of the SITE UNIT parameter was not valid for a PDS (for example, the SITE UNIT was set to TAPE and a PDS cannot be allocated on a tape).

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Issue the SITE command with the UNIT parameter to change the setting of the UNIT parameter to a unit that is valid for a PDS, then reissue the MKD command.

System programmer response

None.

550: MKD failed. Volume for dcbdsn data set *dcbdsn_name* is not mounted and NoAutomount is specified.

Explanation

The MKD command was specified to create a new PDS. The SITE DCBDSN parameter was in effect specifying that all newly created data sets be allocated using data set *dcbdsn_name* as a model data set for the data set characteristics. The volume containing *dcbdsn_name* was not currently mounted to the system, and the FTP server was currently in No AutoMount mode, so the FTP server could not get the

volume mounted to the system to determine the data set characteristics of *dcbdsn_name* to use when allocating the new PDS.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Issue the SITE AUTOMOUNT command to allow the volume containing *dcbdsn_name* to be mounted to the system, then reissue the MKD command.

System programmer response

None.

550: MKD failed. Volume list *volume serial list* includes a volume which is not mounted and NoAutoMount is specified.

Explanation

The client issued the MKD command to create an MVS partitioned data set at the server host. The SITE VOLUME command had previously been issued, or the VOLUME statement was specified in the FTP.DATA file, to specify that all new data sets be allocated on volumes *volume serial list*. Volume list *volume serial list* includes a volume that is not mounted to the system, and NoAutoMount is in effect to prevent the server from automatically requesting the volume to be mounted.

System action

The MKD command is rejected. The FTP server waits for the next command from the client.

User response

If possible, issue the SITE AUTOMOUNT subcommand to allow the FTP server to automatically request the operator to mount every volume in *volume serial list*. Otherwise, contact the MVS System Operator to have the volumes *volume serial list* mounted to the system. Then issue the MKD subcommand again.

System programmer response

If necessary, mount the volumes *volume list* to the system for use.

550: MKD failed. Volume *volume* is not mounted and NoAutoMount is specified.

Explanation

The client issued the MKD command to create an MVS partitioned data set at the server host. Either the SITE VOLUME command was issued, or the VOLUME statement was specified in the FTP.DATA file, to specify that all new data sets be allocated on volume *volume*. Volume *volume* was not mounted to the system, and NoAutoMount is in effect to prevent the server from automatically requesting the volume to be mounted.

System action

The MKD command is rejected. The FTP server waits for the next command from the client.

User response

If possible, issue the SITE AUTOMOUNT subcommand to allow the FTP server to automatically request the operator to mount volume *volume*. Otherwise, contact the MVS System Operator to have the volume *volume* mounted to the system. Then issue the MKD subcommand again.

System programmer response

If necessary, mount the volume *volume* to the system for use.

550: MKD failed. Volume=*serial* is a tape and is invalid for a PDS.

Explanation

The MKD command was issued to create a new PDS. The SITE VOLUME parameter was in effect, specifying that all new data sets be allocated on volume *serial*. *serial* was determined to be a tape, and partitioned data sets cannot be allocated to tape.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Issue the SITE VOLUME command to change or reset the volume serial for new data sets to a direct access volume, then reissue the MKD command.

System programmer response

None.

550: MKD failed. Volume=*volume serial list* includes a tape and is not valid for a PDS.

Explanation

The MKD command was issued to create a new PDS. The SITE VOLUME parameter was in effect, specifying that all new data sets be allocated on volumes *volume serial list*. Or, VOLUME=*volume serial list* was specified in FTP.DATA. The *volume serial list* was determined to include a tape, and partitioned data sets cannot be allocated to tape.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Issue the SITE VOLUME command to change the volume serial for new data sets to one or more direct access volumes. Then the MKD command again.

System programmer response

None.

550: MKD failed. Error mounting dcbdsn data set *dcbdsn_name*.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN parameter was in effect, specifying that all newly allocated data sets should use the data set *dcbdsn_name* as a model data set for the data set characteristics. The volume containing data set *dcbdsn_name* was not currently mounted to the system, and when the FTP server attempted to get the volume mounted, an error occurred and the volume was unable to be mounted. The FTP server was therefore unable to determine the data set characteristics for the new PDS.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Either contact the system programmer for the server system to get the volume containing *dcbdsn_name* mounted (note, the LIST *dcbdsn_name* command will display the volume that contains *dcbdsn_name*), or issue the SITE command to change the model DCB data set specified by the DCBDSN parameter, or use the other SITE parameters to specify the data set characteristics without using a model DCB, then reissue the MKD command.

System programmer response

Determine why the volume containing *dcbdsn_name* cannot be mounted to the system and correct the problem.

550: MKD failed. Error retrieving dcbdsn data set *dcbdsn_name*.

Explanation

The MKD command was issued to create a new PDS. The SITE DCBDSN parameter was in effect, specifying that all newly allocated data sets should use the data set *dcbdsn_name* as a model data set for the data set characteristics. *dcbdsn_name* was migrated, and when the FTP server attempted to recall the data set, an error occurred and the data set was unable to be recalled. The FTP server was therefore unable to determine the data set characteristics for the new PDS.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Either contact the system programmer for the server system to get the *dcbdsn__name* recalled, or issue the SITE command to change the model DCB data set specified by the DCBDSN parameter, or use the other SITE parameters to specify the data set characteristics without using a model DCB, then reissue the MKD command.

System programmer response

Determine why *dcbdsn_name* could not be recalled and correct the problem.

550: MKD failed. Recfm *recfm* is invalid for a PDS.

Explanation

The MKD command was issued to create a new PDS. The SITE RECFM parameter had a value of *recfm*, which is not a valid record format for a PDS.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Issue the SITE RECFM command to change the setting of RECFM to a record format that is valid for a PDS, then reissue the MKD command. (Incorrect record formats are FBS, VBS, and VS).

System programmer response

None.

550: Mkd fails: *new_directory*. User not authorized

Explanation

The MKD command was issued to create the new PDS *new_directory*. However, some part of the high-level qualifiers for *new_directory* were protected by a security system, such as RACF, and the user did not have sufficient authority to create a data set by this name.

System action

The MKD command is rejected. Control is returned to the client connection for further command processing.

User response

Contact the security administrator to get the necessary authorization for creating the data set.

System programmer response

None.

550: MKDIR failed: *error*

Explanation

The client issued a MKD command to create a z/OS UNIX directory at the FTP server host. The C run-time library function mkdir() was issued by the FTP server to create the directory, but the mkdir() function did not complete successfully. *error* is the error message returned by the C run-time library for the failing routine.

System action

The MKD command is rejected. The server waits for the next command from the client.

User response

Reissue the command. If the problem persists, contact the system programmer.

System programmer response

Correct the error indicated by *error*.

550: Name length error for pathname *pathname*

Explanation

The path name provided for a create named pipe request, a data transfer (retrieve or store) request, a delete request, or a rename request is too long. The name, when combined with the current working directory, must adhere to the following maximum lengths:

- 44 for a physical sequential data set
- 54 for a member of a partitioned data set (PDS) (includes the parentheses for the member name)
- 1023 for a file in the z/OS UNIX file system.

Note: The maximum length for a file name is 255. The total path name maximum length is 1023.

In the message text:

pathname
The path name that is too long.

Example

```
Command:
pwd
>>> PWD
257 "'IBMUSER.MAXIMUM.DATASET.NAME.LENGTH.IS44CHAR'" is working directory.
Command:
delete toobig(member)
>>> DELE toobig(member)
550 Name length error for pathname toobig(member)
Command:
```

System action

The request is not performed.

User response

Reissue the request with a name that meets the limits for the type of data set or file.

System programmer response

None.

550: No data sets found.

Explanation

The LIST or NLST command requested a listing of one or more data sets, but the FTP server could not find any data sets that matched the requested pathname.

System action

The LIST or NLST command is rejected.

User response

Verify that the correct data set name or path was entered.

System programmer response

None.

550: No jobs found for JESJOBNAME=*name*, JESSTATUS=*status* and JESOWNER=*owner*

Explanation

No jobs were found that matched the selection criteria specified.

System action

FTP continues.

User response

None.

System programmer response

None.

550: No members found.

Explanation

The LIST or NLST command requested members of a partitioned data set, but no members were found in the PDS that matched the requested name.

System action

The LIST or NLST command is rejected.

User response

Verify that the member name or path was entered correctly.

System programmer response

None.

550: No spool files available for *jobid*

Explanation

User attempted to retrieve spool files from JES and no spool files existed.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the command and reissue.

System programmer response

None.

550: No spool files available for *jobid*, JesPutGet aborted

Explanation

User attempted to retrieve spool files from JES and no spool files were available for processing.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the command and reissue.

System programmer response

None.

550: Non-DASD data set *dsname* cannot be processed.

Explanation

The named data set does not have the correct data set organization. It is neither DASD nor tape.

System action

The data transfer does not occur. FTP continues.

User response

None.

System programmer response

None.

550: Open of *dsname* failed.

Explanation

The data set cannot be opened.

System action

The data set is not sent. FTP continues.

User response

None.

System programmer response

Look at the trace and find the following trace entry sequence:

```
seq_open_file: Ixy  -> r,recfm=* for dsname
seq_open_file: failed (aa): bbbb
```

The first line describes I/O mode as Input with mode values *x* and *y* that are defined as follows:

```
x = S --> stream I/O
x = R --> record I/O

y = B --> binary stream
y = T --> text stream
```

The second line describes error that occurred. *aa* is the errno value returned from the fopen of file. **bbbb** is the text associated with the errno value. The following list describe values and text that could be observed:

(61): Error trying to define file
The file is already opened.

550: Partitioned data set *'pathname'* does not exist

Explanation

The LIST or NLST command requested that members of a partitioned data set be listed, but the requested data set could not be found.

System action

The LIST or NLST command is rejected.

User response

Verify that the PDS name was entered correctly.

System programmer response

None.

550: Pathname does not contain valid Jobid

Explanation

The Jobid was incorrectly specified in the command.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct the request and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: pathname *pathname* not retrievable.

Explanation

The client issued a command command to the FTP server. The FTP server was not able to resolve the pathname, perhaps for one of these reasons:

no pathname was provided;
pathname does not exist;
too many symbolic links had to be resolved to retrieve *pathname*;
pathname contained too many characters to resolve;
the user does not have search permission on some component of *pathname*.

System action

The command is rejected. The FTP server waits for the next command from the client.

User response

Verify you entered the pathname correctly, and that you have access authority to *pathname*. If the commands fails after you have verified *pathname* and access authority, report the error to the system programmer.

System programmer response

Error messages related to *pathname* retrieval are written to syslogd if ftp server traces are enabled. If syslogd is not active, the error messages will be written to the operator console. Fix any problems, and have the user issue the command again.

550: Permanent negative completion.

Explanation

The requested file has a DSORG that is not supported by FTP.

System action

The transfer ends. FTP continues.

User response

None.

System programmer response

None.

550: READTAPEFormat value is *value* but input tape is *format*

Explanation

A GET was issued for a data set on tape and a non-blank value was specified for READTAPEFormat. The READTAPEFormat specification does not match the tape label.

value is one of the following values:

- F — Format was to be fixed .

- V — Format was to be variable.
- S — Format was to be spanned.
- X — Format was to be lrecl X.

If *value* is X, *format* is:

- lrecl *nnnnn* — tape label shows logical record length nnnnn.

If *value* is F, V, or S, *format* is:

- lrecl X — tape label shows lrecl X format.

System action

The request is rejected. FTP continues.

User response

Either specify the matching READTAPEFormat or change it to unspecified and try the request again. See the z/OS Communications Server: IP User's Guide and Commands for the description of the SIte subcommand and for guidelines on using READTAPEFormat.

System programmer response

None.

550: READTAPEFormat *value* is value but input tape is format *format*

Explanation

A GET was issued for a data set on tape and a non-blank value was specified for READTAPEFormat. The READTAPEFormat specification does not match the tape label.

value is one of the following values:

- F — Format was to be fixed.
- V — Format was to be variable.

format is the record format string from the tape label, such as VB, FBA, and so on.

System action

The request is rejected. FTP continues.

User response

Either specify the matching READTAPEFormat or change it to unspecified and try the request again. See the z/OS Communications Server: IP User's Guide and Commands for the description of the SITE command and for guidelines on using READTAPEFormat.

System programmer response

None.

550: READTAPEFormat value is *value* but input tape is not spanned.

Explanation

A GET was issued for a data set on tape and a non-blank value was specified for READTAPEFormat. The READTAPEFormat specification does not match the tape label.

value is one of the following values:

- S — Format was to be spanned.

System action

The request is rejected. FTP continues.

User response

Either specify the matching READTAPEFormat or change it to unspecified and try the request again. See the z/OS Communications Server: IP User's Guide and Commands for the description of the SITE command and for guidelines on using READTAPEFormat.

System programmer response

None.

550: READTAPEFormat value is *value* but input tape is spanned

Explanation

A GET was issued for a data set on tape and a non-blank value was specified for READTAPEFormat. The READTAPEFormat specification does not match the tape label.

value is one of the following values:

- F — Format was to be fixed.
- V — Format was to be variable.

System action

The request is rejected. FTP continues.

User response

Either specify the matching READTAPEFormat or change it to unspecified and try the request again. See the z/OS Communications Server: IP User's Guide and Commands for the description of the SITE command and for guidelines on using READTAPEFormat.

System programmer response

None.

550: Rename fails: *dsname* already exists.

Explanation

The RNTO command was issued to rename a data set. A data set already exists with the new name.

System action

The data set is not renamed. FTP continues.

User response

Either delete the existing data set or choose a different new name.

System programmer response

None.

550: Rename fails: GDG name conversion failed.

Explanation

The relative name for a Generation Data Group (GDG) data set could not be converted into its absolute form.

System action

The request is not performed.

User response

Ensure that the name provided is the name of an existing GDG data set (for the old name) or that the new name specifies an exiting base name for a GDG.

System programmer response

None.

550: Renaming attempt failed. Rc was *errno*

Explanation

The RNTO command was issued to rename a data set. The rename was unsuccessful.

System action

The data set is not renamed. FTP continues.

User response

None.

System programmer response

The return code *errno* is the errno value received when the rename C function was invoked to rename the data set. *errno* is the UNIX System Services Return Code. These return codes are listed and described in the z/OS UNIX System Services Messages and Codes.

550: Request nonexistent member *file_name* to be sent.

Explanation

The member that was named is not a member of the partitioned data set (PDS) and cannot be retrieved.

file_name is the name of the partitioned data set.

System action

The data set is not sent. FTP continues.

User response

Reissue the command with the corrected PDS or member name.

System programmer response

None.

550: request size of nonexistent member *member*

Explanation

The FTP server received a SIZE *file name* request. The *file name* specifies a partitioned data set member that does not exist.

System action

The SIZE command is rejected. The FTP server waits for the next command.

User response

Issue the SIZE command with a correct file name.

System programmer response

None.

550-: Request to export security context failed

Explanation

The server call to the gss_export_sec_context() function failed. This reply is preceded by replies specifying the return codes returned from the failing function call. See those replies for further diagnosis.

System action

FTP ends.

User response

None.

System programmer response

See z/OS Integrated Security Services Network Authentication Service Programming for an explanation of the gss_export_sec_context() function.

550: Retrieval of a whole partitioned data set is not supported. Use MGET or MVSGET for this purpose.

Explanation

The data set that was named is a partitioned data set (PDS) and cannot be retrieved as a single file.

System action

The data set is not sent. FTP continues.

User response

To get the whole data set, retrieve all members of the data set. For example, use the MGET or MVSGET client subcommand if available. For more information about the z/OS FTP MGet and MVSGet subcommands, see FTP subcommands in z/OS Communications Server: IP User's Guide and Commands.

System programmer response

None.

550: RMD failed. Valid only for z/OS UNIX files or partitioned data sets.

Explanation

The RMD command was issued to remove a directory, but the directory name entered was not a valid PDS or z/OS UNIX directory.

System action

FTP continues

User response

Re-issue the command with the correct directory name.

System programmer response

None.

550: Rmd fails: *directory*. User not authorized

Explanation

The RMD command was issued to delete the partitioned data set *directory*, but *directory* was protected by a security system such as RACF and the user was not authorized to delete the data set.

System action

The RMD command is rejected. Control returns to the client for further command processing.

User response

Contact the owner of the data set to get the necessary authorization to delete the data set.

System programmer response

If required, authorize the user to delete the partitioned data set.

550: RMDIR failed: *error*

Explanation

The client issued a RMD command to delete a z/OS UNIX directory at the FTP server host. The C run-time library function rmdir() was issued by the FTP server to delete the directory, but the rmdir() function did not complete successfully. *error* is the error message returned by the C run-time library for the failing routine.

System action

The RMD command is rejected. The server waits for the next command from the client.

User response

Reissue the command. If the problem persists, contact the system programmer.

System programmer response

Correct the error indicated by *error*.

550: RNFR fails: *dsname* does not exist.

Explanation

The RNFR command was issued to rename a data set. The rename was unsuccessful because the data set does not exist.

System action

FTP continues.

User response

Make sure that the correct data set name is entered and that the data set is catalogued.

System programmer response

None.

550: RNFR fails: *dsname*. User not authorized.

Explanation

The RNFR command was issued to rename a data set. The requested data set is protected by a security system such as RACF, and the user is not authorized to rename the data set.

System action

The data set is not renamed. FTP continues.

User response

Contact the owner of the data set for authorization to rename it.

System programmer response

None.

550: RNTO fails: *dsname*. User not authorized.

Explanation

The RNTO command was issued to rename a data set. The requested data set is protected by a security system such as RACF, and the user is not authorized to rename the data set.

System action

The data set is not renamed. FTP continues.

User response

Contact the owner of the data set for authorization to rename it.

System programmer response

None.

550 : SIZE command not supported with active security mechanism

Explanation

The SIZE command is not supported when the connection is protected by a security mechanism.

System action

The SIZE command fails. FTP continues.

User response

None.

System programmer response

None.

550: Size of a whole Partitioned data set is not supported

Explanation

The FTP server received a SIZE command that specified an entire partitioned data set. Partitioned data sets cannot be transferred as a single file. SIZE is not supported for data sets that cannot be transferred.

System action

No SIZE information is sent. The FTP server waits for the next command.

User response

To approximate the byte transfer size of a partitioned data set, issue SIZE for each member, then add the sizes together. To transfer the partitioned data set, you would have to transfer each member and aggregate them at the client.

System programmer response

None.

550: SIZE fails: *file name* is migrated

Explanation

The FTP server received a SIZE *file name* request. The *file name* specifies a data set that was migrated. SIZE is not supported for migrated data sets.

System action

The SIZE command is rejected. The FTP server waits for the next command.

User response

Ask the MVS operator to recall the data set. Then issue the SIZE command again.

System programmer response

None.

550: SIZE fails: *filename* is on a volume which is not mounted

Explanation

The FTP server received a SIZE *file name* request. The *file name* specifies a data set on a volume that is not mounted. SIZE is not supported for data sets on volumes that are not mounted.

System action

The SIZE command is rejected. The FTP server waits for the next command.

User response

Ask the MVS operator to mount the required volume. Then issue the SIZE command again.

System programmer response

None.

550: SQL query not available. Can't load CAF routines.

Explanation

FTP was unable to load the CAF (Call Access Facility) modules it uses to provide support for SQL queries.

System action

The command is rejected. FTP continues.

User response

If FTP SQL support should be available, contact your system programmer. If FTP SQL support was not intended, issue a 'SITE filetype=' command to change the filetype from its current setting of 'SQL' to 'SEQ' or 'JES'.

System programmer response

If FTP SQL support is desired, ensure that the appropriate DSNLOAD library is included in the STEPLIB for the FTP server. (If FTP is started from the z/OS UNIX shell, the $STEPLIB environment variable must be set.) Restart the FTP server.

550-: SVC99 RETURN CODE=*rc* S99INFO=*info* S99ERROR=*decerr* HEX=*hexerr* S99ERSN code *code*.

Explanation

module SVC99 passed back a nonzero return code. This message documents the return code, S99INFO and S99ERROR values.

rc is the return code.

info is the information code.

decerr is the error code in decimal.

hexerr is the error code in hexadecimal.

code is the reason code in hexadecimal.

System action

The file transfer will end if the data set was not allocated.

User response

Determine why the data set was not allocated, correct as necessary, and try again. See the z/OS MVS Programming: Authorized Assembler Services Guide for information about interpreting DYNALLOC return codes.

System programmer response

Determine why the data set was not allocated and correct.

550-: System completion code and reason: *code-reason*

Explanation

While the FTP server was processing a command from the FTP client, the server experienced an abend.

In the message text:

code
The system completion code associated with the abend.

reason
The reason code associated with the system completion code.

Example

```
Command:
delete etchost
>>>DELE etchost
550-System completion code and reason: 213-50
550 could not delete USER5.PDS(ETCHOST)
Command:
```

System action

The FTP server stops processing the current command.

Operator response

Save the system log for problem determination and report the error to the system programmer.

User response

Report the code and reason values to the system programmer.

System programmer response

See z/OS MVS System Codes for suggested actions for the specified system completion code.

Problem determination

See the system programmer response.

Source

z/OS Communications Server TCP/IP: FTP

Module

ezaftprf.c

550: TAPEREADSTREAM does not support transfer of an American Standards Association (ASA) data set

Explanation

The server received an RETR command to retrieve an ASA tape data set when the server was configured with **TAPEREADSTREAM=TRUE**.

System action

The RETR command is rejected.

User response

If your client is a z/OS Communications Server FTP client, issue a SITE NOTAPEREADSTREAM subcommand to change the value for the current session. If your client is not a z/OS Communications Server FTP client, issue a QUOTE SITE NOTAPEREADSTREAM subcommand to change the value for the current session. For more information about the SIte subcommand, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

To change the TAPEREADSTREAM value permanently, change the TAPEREADSTREAM statement in FTP.DATA. For more information about the TAPEREADSTREAM statement, see z/OS Communications Server: IP Configuration Reference.

550: TAPEREADSTREAM does not support transfer of the trailing blanks in a fixed format tape data set

Explanation

The server received an RETR command to retrieve a fixed format tape data set when the server was configured with **TAPEREADSTREAM=TRUE** and **TRAILINGBLANKS=TRUE**.

System action

The RETR command is rejected.

User response

If your client is a z/OS Communications Server FTP client, issue a SITE NOTAPEREADSTREAM or SITE NOTRAILINGBLANKS subcommand to change the value for the current session. If your client is not a z/OS Communications Server FTP client, issue a QUOTE SITE NOTAPEREADSTREAM or QUOTE SITE NOTRAILINGBLANKS subcommand to change the value for the current session. Fore more information about the SIte subcommand, see z/OS Communications Server: IP User's Guide and Commands.

System programmer response

To change the TAPEREADSTREAM or NOTRAILINGBLANKS value permanently, change the TAPEREADSTREAM or TRAILINGBLANKS statement in FTP.DATA. For more information about the TAPEREADSTREAM or TRAILINGBLANKS statement, see z/OS Communications Server: IP Configuration Reference.

550: The user is not authorized to access the job

Explanation

A DELETE command was issued to a job the issuer does not have appropriate authority.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Correct and reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Transfer aborted

Explanation

This is the final reply of a group of replies.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

See replies prior to the 550 reply.

System programmer response

None.

550: TYPE U transfer requires variable format data set

Explanation

You attempted to put a data set while the transfer type is Unicode and the record format was not variable.

System action

The request is rejected. FTP continues.

User response

Change the record format to variable (SITE RECFM)

System programmer response

None.

550: Unable to append to *dsname*

Explanation

An internal error occurred during the processing of the append request.

System action

The request is not performed.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

550: Unable to append to fixed record format file in image mode

Explanation

The server does not supports an append request for a fixed format file when the data type is image.

System action

The append is not performed.

User response

Reissue the request with data type ASCII or EBCDIC.

System programmer response

None.

550: Unable to append to member *name* in Partitioned data set *dsname*

Explanation

An internal error occurred while trying to process a data set.

System action

The request is not performed.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

550: Unable to append to the Null directory.

Explanation

The current working directory is the null directory. The server does not support the append command to the null directory.

System action

The command is rejected. FTP continues.

User response

Use the STOR or STOU command to store to the null directory or change the directory to use append.

System programmer response

None.

550: Unable to create data set *dsname* for *command* command.

Explanation

The server attempted to allocate to a new data set to store data. The dynamic allocation was unsuccessful. *command* is STOR, STOU, or APPE.

System action

The command is rejected. FTP continues.

User response

None.

System programmer response

Examine the trace and look for trace messages with the tag *seq_create_file*. These trace messages provide the reason codes for the dynamic allocation error.

550: Unable to delete *directory* (Error code: *error_code*, Reason code: *reason_code*, S99ERSN code *s99reason_code*).

Explanation

The RMD or DELE command was issued to delete PDS *directory*, but when the FTP server attempted to delete the data set, the delete did not complete successfully. Possible causes for this error include the data set is currently in use by someone else, the data set has an unexpired retention period, the data set is located on a tape volume, or the direct access volume containing the data set is not writable.

System action

The RMD or DELE command is rejected. Control returns to the client for further command processing.

User response

Reissue the command. If the problem persists, contact the system programmer for the server system.

System programmer response

The *error_code*, *reason_code*, and *s99reason_code* values displayed contain the S99ERROR, S99INFO, and S99ERNS fields from DYNALLOC. See Interpreting DYNALLOC return codes in the z/OS MVS Programming: Authorized Assembler Services Guide to determine why the data set cannot be deleted and correct the problem.

550: Unable to delete *dsname* (Rc = *errno*).

Explanation

The attempt to delete a z/OS UNIX file was unsuccessful.

System action

The file is not deleted. FTP continues.

User response

None.

System programmer response

The return code *errno* is received when the remove C function was invoked to delete the file. *errno* is the UNIX System Services Return Code. These return codes are listed and described in the z/OS UNIX System Services Messages and Codes.

550: Unable to obtain data set list

Explanation

A service call was issued to obtain the list of requested data sets from the MVS system, but the service call was unsuccessful.

System action

The LIST or NLST command is rejected.

User response

Try the command again. If the problem persists, contact the system programmer for the FTP server system.

System programmer response

If necessary, re-create the problem with FTP server traces turned on. Locate the last occurrence of the trace message “list2: return code *rc* from gtlist.”. This trace message will contain the return code from the service call that was unsuccessful. Determine the cause and correct the problem.

550-: Unable to obtain JES NODE name from subsystem information

Explanation

The FTP server was attempting to use the JES SubSystem Interface (SSI54) to obtain the JES home NODE name, but the information was not available.

System action

No data is sent. FTP continues.

User response

Ensure that the JES subsystem is active.

System programmer response

None.

550: Unable to perform LIST/NLST command due to error with /dev/null.

Explanation

During server initialization, the server attempted to open STDOUT and STDERR to the /dev/null character special file. It was unable to do so, and the server is not able to perform the LIST or NLST subcommand for z/OS UNIX files.

System action

The command is rejected. FTP continues.

User response

Contact the system programmer.

System programmer response

Error Message EZYFT48E logged during server initialization will contain the reason for the /dev/null failure. Correct this error and restart the FTP server.

550: Unable to send *dsname*

Explanation

The named data set is for a generation data group (GDG) that does not exist.

System action

The data set is not sent. FTP continues.

User response

Ensure that the GDG exists.

System programmer response

None.

550: Unable to size *dsname*

Explanation

An error occurred while the FTP server was trying to determine the byte transfer size of of *dsname*.

System action

No size information is returned for *dsname*. FTP continues.

User response

Report the error to the system programmer.

System programmer response

Error messages related to *dsname* are written to syslogd if ftp server traces are enabled. If syslogd is not active, the error messages will be written to the operator console.

550: Unable to store *dsname*

Explanation

An internal error occurred during the processing of the store request.

System action

The request is not performed.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

550: Unable to store member *name* in Partitioned data set *dsname*

Explanation

An internal error occurred during the processing of the store request.

System action

The request is not performed.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

550: Unable to store unique *dsname*

Explanation

An internal error occurred during the processing of the store unique request.

System action

The request is not performed.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

550: Unable to store unique member *name* in Partitioned data set *dsname*

Explanation

An internal error occurred while trying to process a data set.

System action

The request is not performed.

User response

Contact the system programmer.

System programmer response

Contact the IBM Support Center.

550: Unexpected status for *dsname*

Explanation

An unexpected error occurred attempting to locate a data set.

System action

The request is not performed.

User response

Ensure that the characteristics of the dataset in question are valid. Also, ensure that the data set characteristics passed on the SITE command or the defaults specified in the FTP.DATA file are valid.

System programmer response

Contact the IBM Support Center.

550: Unknown HOME directory for pathname *path*

Explanation

A command was issued that required the server to resolve the user's HOME directory name (for example, a pathname was entered that began with the directory notation ~/) but the server was unable to determine the user's HOME directory.

System action

The command is rejected. FTP continues.

User response

Verify that the OMVS user ID has a HOME directory. If necessary, define a HOME directory for the user ID.

System programmer response

None.

550: Unknown return code from Get JES spool request: *number*

Explanation

During the processing of a JES request, an unknown return code was returned from JES.

System action

Unpredictable results might occur.

User response

Issue the command again. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Unknown return code from Get JES spool request: *number*, JesPutGet aborted

Explanation

During the processing of a JES request, an unknown return code was returned from JES.

System action

Unpredictable results might occur.

User response

Issue the request again. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Unknown return code from JES cancel request

Explanation

A request was made to delete a job from JES. During the processing of this request, JES provided an unknown return code.

System action

Unpredictable results might occur.

User response

Issue the request again. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: User Exit refuses this Job to be submitted by *dsname*

Explanation

During the submit of a job to JES, a JES user or installation exit encountered an error. The request to submit the job might have failed.

System action

FTP server continues normal execution. The FTP client waits for the next command input.

User response

Reissue the command. If problem persists, contact appropriate support personnel.

System programmer response

Diagnose the problem.

550: Volume containing *dsname* is not mounted and NoAutoMount specified.

Explanation

The command requested MVS data set *dsname*, but the volume containing *dsname* was not mounted to the system and the FTP server was currently in No Automount mode.

System action

The command is rejected.

User response

If possible, issue the SITE AUTOMOUNT command to allow the volume containing the data set to be automatically mounted; otherwise, contact the system operator to mount the volume to the system. Then reissue the command.

System programmer response

None.

550-: volume for "*new_directory*" is not mounted and NoAutomount is specified

Explanation

The volume containing the requested *new_directory* was not mounted and the server was currently in No AutoMount mode. Therefore, the server could not mount the volume to complete the CWD command.

System action

The CWD command is rejected.

User response

If possible, issue the SITE AUTOMOUNT command to allow the server to request automatic volume mounts. Otherwise, issue the STAT command to find the current value for VOLUME. Ask the MVS operator to mount the indicated volume or volumes; then issue the MKD command again.

System programmer response

If necessary, have the volume mounted to the system.

550: Volume is not ready and automatic tape mounts are not allowed.

Explanation

A request to retrieve a data set from or store a data set on a tape volume was received. The tape volume is not mounted and the end user requested NoAutoTapeMount.

System action

The request is not performed.

User response

Request that the tape be mounted by the operator and then reissue the request. Also, the SITE AUTOTAPEMOUNT subcommand can be issued to allow automatic tape mounts to occur.

System programmer response

None.

550: Volume *name* is not mounted and NoAutoMount is specified.

Explanation

A store request was received for which a new data set must be created. The volume on which the data set was to be created is not mounted and the server was currently in NoAutoMount mode.

System action

The request is not performed.

User response

Request that the volume be mounted by the operator and then reissue the request. Also, the SITE AUTOMOUNT subcommand can be issued to allow automatic DASD mounts to occur.

System programmer response

None.

550: Volume=*volume list* includes a volume which is is not mounted and NoAutoMount is specified.

Explanation

The FTP server received a store request that required it to create a new data set. All the volumes in *volume list* are needed to create the new data set. One or more of the volumes is not mounted and the server is currently in NoAutoMount mode.

System action

The FTP server rejects the request. The server waits for the next command.

User response

If possible, issue SITE AUTOMOUNT to allow the server to request volume mounts automatically. Otherwise, ask the MVS operator to mount all the volumes in *volume list*.

System programmer response

None.

550: VSAM data set *dsname* cannot be processed.

Explanation

The named data set is a VSAM data set and cannot be processed.

System action

The data set is not sent. FTP continues.

User response

None.

System programmer response

None.

551 reply codes

551: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The command in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

551: Reload of the load library failed

Explanation

While processing a PUT or MPUT command for one or more load modules, the server failed to reload the load modules from the temporary data set into the load library. The transfer is ended, and no files will be transferred.

System action

FTP waits for the next command.

User response

Contact your system programmer.

System programmer response

Verify sufficient free space exists in the load library to receive the load modules. Look for console messages from file system or the IEBCOPY utility. Get a server trace of the operation.

551: Transfer aborted: attempt to connect to *db2name* failed *(code)*

Explanation

FTP attempted to process a SQL request, but was unable to connect to the Db2 subsystem named *db2name*.

System action

No data is sent. FTP continues.

User response

If the Db2 subsystem name *(db2name)* is incorrect, issue a 'SITE db2=' command for the correct Db2 subsystem name, and resubmit the SQL query. If the Db2 subsystem name is correct, contact your system programmer for FTP.

System programmer response

Ensure that the Db2 subsystem was started. See the *Db2 Messages and Codes* for a detailed explanation of *code*.

551: Transfer aborted: *condition* occurred for TYPE U transfer

Explanation

The transfer of data ended because of an error reading the data set.

System action

FTP continues.

User response

None.

System programmer response

Get a trace of the retrieve operation and contact the IBM Software Support Center.

551: Transfer aborted: conversion failure

Explanation

The transfer of data ended because of an error reading the data set.

System action

FTP continues.

User response

None.

System programmer response

Get a trace of the retrieve operation and contact the IBM Software Support Center.

551: Transfer aborted: internal read error.

Explanation

The transfer of data ended because an internal error was detected while attempting to read the data.

System action

FTP continues.

User response

None.

System programmer response

Get a trace of the operation and contact the IBM Software Support Center.

551: Transfer aborted: internal write error.

Explanation

The transfer of data ended because an internal error was detected while attempting to write the data.

System action

FTP continues.

User response

None.

System programmer response

Get a trace of the operation and contact the IBM Software Support Center.

551: Transfer aborted: SQL CURSOR DECLARE failure

Explanation

Db2 encountered an error while processing a SQL statement submitted through FTP. The FTP output file contains the error message from Db2.

System action

FTP continues.

User response

If possible, correct the error indicated in the output file and resubmit the SQL request. Otherwise, contact your system programmer for FTP.

System programmer response

Correct the error indicated by the message contained in the output file. For detailed explanation of Db2 error codes, see the *Db2 Messages and Codes*.

551: Transfer aborted: SQL CURSOR OPEN failure

Explanation

Db2 encountered an error while processing a SQL statement submitted through FTP. The FTP output file contains the error message from Db2.

System action

FTP continues.

User response

If possible, correct the error indicated in the output file and resubmit the SQL request. Otherwise, contact your system programmer for FTP.

System programmer response

Correct the error indicated by the message contained in the output file. For detailed explanation of Db2 error codes, see the *Db2 Messages and Codes*.

551: Transfer aborted: SQL not available. Attempt to open plan *plan_name* failed *(code)*

Explanation

FTP attempted to process a SQL request, but was unable to open FTP's Db2 subsystem plan named *plan_name*

System action

No data is sent. FTP continues.

User response

If FTP SQL support should be available, contact your system programmer for FTP. If a SQL query was not intended, issue 'SITE filetype=' command to change the filetype from 'SQL' to 'SEQ' or 'JES' before the next FTP retrieve command.

System programmer response

Ensure that a BIND was done for plan *plan name* and that execute authorization was granted for the plan.

Note: If you used a plan name other than EZAFTPMQ for the EZAFTPMQ DBRM, your FTP.DATA file must contain a DB2PLAN statement to specify the plan name that the FTP server is to use. See *Db2 Messages and Codes* for a detailed explanation of *code*.

551: Transfer aborted: SQL PREPARE/DESCRIBE failure

Explanation

Db2 encountered an error while processing a SQL statement submitted through FTP. The FTP output file contains the error message from Db2.

System action

FTP continues.

User response

Correct the error indicated in the output file, and resubmit the SQL request.

System programmer response

None.

551: Transfer aborted: uneven number of bytes received for TYPE U transfer

Explanation

The transfer of data ended because of an error reading the data set.

System action

FTP continues.

User response

None.

System programmer response

Get a trace of the retrieve operation and contact the IBM Software Support Center.

551: Unload of the load library failed

Explanation

While processing a GET or MGET command for one or more load modules, the server failed to unload the load modules into a temporary data set. The transfer is ended, and no files will be transferred.

System action

FTP waits for the next command.

User response

Contact your system programmer.

System programmer response

Verify sufficient free space exists on the file system to receive the temporary data set. Look for console messages from file system or the IEBCOPY utility. Get a server trace of the operation.

552 reply codes

552: Command *cmd* fails: *filename* does not exist.

Explanation

The server received a *cmd* command with *filename* as a parameter. The *filename* file does not exist.

In the message text:

cmd
The FTP command that the server received .

filename
The file or data set name that is specified on the FTP command.

Example

```
mvsput 'user1.ftp.ps'
'user1.ftp.noexist'
```

```
quote xdss 'user1.ftp.noexist'
EZA1701I >>> xdss  'user1.ftp.noexist'
552 Command XDSS fails - USER1.FTP.NOEXIST does not exist.
EZA1701I >>> SITE DSNTYPE=BASIC RECFM=VB BLKSIZE=6233 LRECL=256 PRIMARY=1 SECOND
ARY=1 EATTR=SYSTEM TRACKS
200 SITE command was accepted
```

System action

The command is rejected. FTP continues processing.

Operator Response

No action is needed.

User response

- If reply code 552 is the expected result for *cmd*, no action is needed.
- If reply code 552 is not the expected result for *cmd*, reissue the FTP subcommand that sent the *cmd* command to the server and specify an existing file or data set.

System programmer response

No action is needed.

Problem Determination

Not applicable.

554 reply codes

554: command terminated due to server shutdown in progress

Explanation

The FTP server was processing a command from the client when the process was stopped either by an OMVS **kill** command, or by a server abend. The server has begun shutdown processing.

System action

The subcommand in progress and the FTP server session process ends.

User response

None.

System programmer response

If the server process was stopped due to an abend, contact the IBM Support Center.

554: Multibyte transfer not supported for destination processing

Explanation

The FTP client attempted to send a file to a Network Job Entry (NJE) destination while Encoding was set to Multi Byte Character Set (MBCS), which is not supported.

See DEST statement (FTP Server) in z/OS Communications Server: IP Configuration Reference for more information about destination processing. See Encoding statement (FTP Client and Server) in z/OS Communications Server: IP Configuration Reference for more information about encoding.

System action

The transfer fails. The FTP server waits for the next command.

User response

If the file you want to transfer is a Single Byte Character Set (SBCS) file, you can send a SITE ENCODING=SBCS command to the server and send the file again. If your client is z/OS FTP, use the SIte subcommand to send a SITE command to the server. See the SIte subcommand in z/OS Communications Server: IP User's Guide and Commands for more information.

System programmer response

None.

554: Requested action not taken: file not found.

Explanation

A restart request was received for the FTP server to resume storing into a data set or file at a point indicated by a restart marker. The data set or file does not exist so the restart is not possible.

System action

FTP continues.

User response

System programmer response

554: Requested action not taken: GDG name conversion failed.

Explanation

A request was received to store a relative generation number of a Generation Data Group (GDG) data set. The relative name could not be converted into an absolute name.

System action

FTP continues.

User response

Ensure that the data set name is a valid generation data group.

System programmer response

None.

554: Requested action not taken: invalid REST parameter.

Explanation

A RETR command is being processed as part of a restart of a checkpointed command. Before the RETR was sent, a REST command was processed and a restart marker was saved. The restart marker is incorrect.

System action

The RETR command is rejected.

User response

None.

System programmer response

Look at the trace to determine the error that occurred when the repositioning was done.

554: Restart not valid for destination processing

Explanation

The user attempted a **restart** or **srestart** FTP subcommand after a site dest=*destination* subcommand had been issued. **Restart** and **srestart** are not valid while a site dest=*destination* option is in effect.

System action

FTP stops processing the restart or srestart subcommand and prompts for the next subcommand.

User response

If a SITE DEST=*destination* subcommand was issued before the file transfer you are trying to restart failed, you cannot restart the file transfer. Issue a get or put subcommand to transfer the file or data set. If no SITE DEST=*destination* subcommand was issued when the original file transfer failed, issue SITE DEST to rescind the SIte subcommand. Issue **restart** or **srestart** again.

System programmer response

None.

554: Transfer aborted: unsupported SQL statement

Explanation

FTP retrieved a file (or data set) while filetype = "SQL' but the contents of the file contain a SQL statement that is not supported by FTP.

System action

The RETR command is rejected.

User response

If a SQL query was intended, reissue the RETR command for a file that contains a SQL SELECT statement. If SQL query was not intended, issue a 'SITE filetype=' command to change the current setting of filetype to either 'SEQ' or 'JES'.

System programmer response

None.

557 reply codes

557 : Data contains codepoints that cannot be translated

Explanation

The data cannot be translated using the current translate table. The translate table was built from the code sets that are specified by the SBDATACONN parameter on SITE or an SBDATACONN statement in the FTP.DATA file. At the time the table was built, one or more of the codepoints was reported as untranslatable for specific data codepoints. The data in this transfer has one or more of the codepoints.

System action

FTP continues.

User response

Use SITE SBDATACONN to build or select a translation table that can translate the codepoints in the data

System programmer response

None.

557 : File contains ASCII data - enter TYPE A command before entering *cmdname* command

Explanation

The FTP server determined that the local file is tagged as an ASCII file. FTP will process this file only if the data type is set to ASCII.

cmdname is either RETR or SIZE.

System action

FTP continues.

User response

Issue the TYPE A command and re-issue the command that failed.

System programmer response

None.

557 : File contains binary data - enter TYPE I command before entering *cmdname* command

Explanation

The FTP server determined that the local file is tagged as a binary file. FTP will process this file only if the data type is set to binary.

cmdname is either RETR or SIZE.

System action

FTP continues.

User response

Issue the TYPE I command and re-issue the command that failed.

System programmer response

None.

557 : JES functions are not allowed with ASCII codepage *codepage*

Explanation

The current codepage specified for the file system by an SBDATACONN statement in the FTP.DATA file or by the SBDATACONN parameter on a SITE command is an ASCII codepage. JES functions cannot be performed if the file system codepage name is an ASCII codepage.

codepage is the name of the current codepage.

System action

FTP continues.

User response

Use a SITE SBDATACONN command to specify a file system codepage that is EBCDIC or use SITE SBDATACONN command to choose a data set for the translation table.

System programmer response

None.

Chapter 18. Intrusion detection services probeids

Intrusion Detection Services defines a code called a probeid to identify the reason and code location associated with output information. The probeids appear in IDS console messages, IDS syslogd messages, packets traced in the SYSTCPIS portion of the stack dataspace and CTRACE records in the SYSTCPIP portion of the stack dataspace.

IDS probeids are four bytes in length. The first byte indicates the IDS type:

- X'01' TCP Traffic Regulation event
- X'02' UDP Traffic Regulation event
- X'03' Scan detection event
- X'04' Attack detection event

The second byte is based on the IDS type. For the Traffic Regulation probeids, the second byte is always zero.

- For Scan detection probeids, a nonzero value in the second byte indicates the suspicion level assigned to a packet being tracked. The following list shows the possible values:
  - X'01' for very suspicious packet.
  - X'02' for possibly suspicious packet.
  - X'03' for normal packet.
  - X'00' is used to report a scan detected event or other unusual situation that might affect scan processing. These conditions are not written to the IDS trace but are written to the syslogd or the console if requested by the policy.
- For Attack detection, the second byte of the probeid identifies the attack type.
  - X'01' MALFORMED_PACKET
  - X'02' OUTBOUND_RAW
  - X'03' IP_FRAGMENT
  - X'04' ICMP_REDIRECT
  - X'05' RESTRICTED_IP_OPTIONS
  - X'06' RESTRICTED_IP_PROTOCOL
  - X'07' FLOOD
  - X'08' PERPETUAL_ECHO
  - X'09' DATA_HIDING
  - X'0A' TCP_QUEUE_SIZE
  - X'0B' GLOBAL_TCP_STALL
  - X'0C' OUTBOUND_RAW_IPV6
  - X'0D' RESTRICTED_IPV6_NEXT_HDR
  - X'0E' RESTRICTED_IPV6_DST_OPTIONS
  - X'0F' RESTRICTED_IPV6_HOP_OPTIONS
  - X'10' EE_LDLC_CHECK
  - X'11' EE_MALFORMED_PACKET
  - X'12' EE_PORT_CHECK
  - X'13' EE_XID_FLOOD
  - X'00' is used to report an attack detected event or other unusual situation that might affect attack processing.

© Copyright IBM Corp. 2000, 2021

Table 26. Intrusion detection services probeids	
probeid	**description**
X'01000001'	TCP TR, enter constrained for receive queue.
X'01000002'	TCP TR, exit constrained for receive queue.
X'01000003'	TCP TR, enter constrained for send queue.
X'01000004'	TCP TR, exit constrained for send queue.
X'01002200'	TCP TR, enter or leave constrained during close processing.
X'01002400'	TCP TR, enter or leave constrained during close processing.
X'01004014'	TCP TR, source host allowed to exceed the percentage of available connections allowed for a single source because of QoS policy.
X'01004042'	TCP TR, source host exceeded both the percentage of available connections allowed for a single source and QoS policy.
X'01004044'	TCP TR, source host exceeded the percentage of available connections allowed for a single source.
X'01004048'	TCP TR, destination port exceeded the total number of connections limit.
X'01004084'	TCP TR, internal error processing source host hash table.
X'01004088'	TCP TR, internal error processing destination port hash table.
X'01004200'	TCP TR, enter or leave constrained during connection handshake complete processing.
X'01004400'	TCP TR, enter or leave constrained during connection handshake complete processing.
X'01004800'	TCP TR, enter or leave constrained during connection handshake complete processing.
X'01008400'	TCP TR, enter or leave constrained during listen processing.
X'01008800'	TCP TR, enter or leave constrained during listen processing.
X'0100C800'	TCP TR, enter or leave constrained during policy change processing.
X'0100FFF0'	TCP TR, log records suppressed.
X'0100FFF1'	TCP TR, Event recording capacity exceeded and TCP TR log records lost.
X'0100FFF2'	TCP TR, Event recording capacity exceeded and TCP TR statistics records lost.
X'02000001'	UDP TR port entered constrained state.
X'02000002'	UDP TR port exited constrained state.
X'02000003'	UDP TR port exited constrained state at policy end.
X'02000004'	UDP TR port IDS Packet traced during constrained state.
X'0200FFF1'	UDP TR, Event recording capacity exceeded and UDP TR log records lost.
X'0200FFF2'	UDP TR, Event recording capacity exceeded and UDP TR statistics records lost.
X'0300FFF1'	Scan, Fast scan detected.
X'0300FFF2'	Scan, Slow scan detected.
X'0300FFF3'	Scan, Scan processing encountered a storage constraint.
X'0300FFF4'	Scan, Scan storage constraint exited.
X'0300FFF5'	Scan, Scan internal interval overrun.

Table 26. Intrusion detection services probeids (continued)	
probeid	**description**
X'0300FFF6'	Scan, Scan detail.
X'0300FFF7'	Scan, Event recording capacity exceeded and Scan log records lost.
X'0300FFF8'	Scan, Event recording capacity exceeded and Scan Detail log records lost.
X'03010001'	Scan, Very Suspicious, request issued to a Reserved port.
X'03010011'	Scan, Very Suspicious, ICMP request to broadcast or multicast address.
X'03010021'	Scan, Very Suspicious, half open connection timed out.
X'03010025'	Scan, Very suspicious, unexpected TCP flags or flag combinations (such as syn and fin both set).
X'03010028'	Scan, Very suspicious, no peer connection and unexpected TCP flags set.
X'03010030'	Scan, Very suspicious, ICMPv6 Echo request to multicast address.
X'03020002'	Scan, Possibly suspicious, request to an Unbound port.
X'03020004'	Scan, Possibly suspicious, rejected by IP Security.
X'03020005'	Scan, Possibly suspicious, no peer connection and rejected by IP Security.
X'03020006'	Scan, Possibly suspicious, unexpected state.
X'03020012'	Scan, Possibly suspicious, ICMP Info request.
X'03020013'	Scan, Possibly suspicious, ICMP Subnet mask request.
X'03020014'	Scan, Possibly suspicious, ICMP request with Record Route option.
X'03020015'	Scan, Possibly suspicious, ICMP request with Record Timestamp option.
X'03020020'	Scan, Possibly suspicious, reset to half open TCP connection.
X'03020024'	Scan, Possibly suspicious, TCP connection timed out.
X'03020026'	Scan, Possibly suspicious, TCP syn dropped.
X'03020027'	Scan, Possibly suspicious, no TCP connection.
X'03020031'	Scan, Possibly suspicious, ICMPv6 Echo request with Routing header.
X'03030000'	Scan, Normal packet. For example, normal TCP connection completed or ICMP echo request to a single host without special options.
X'03030003'	Scan, Rejected by QOS policy.
X'03030007'	Scan, Normal packet. UDP normal packet.
X'03030022'	Scan, Out of sequence window.
X'03030023'	Scan, Stand alone syn but connection already established.
X'03030026'	Scan, TCP syn dropped.
X'0400FFF1'	Attack, Event recording capacity exceeded and Attack log records lost.
X'0400FFF2'	Attack, Event recording capacity exceeded and Attack statistics records lost.
X'04010001'	Attack, type=MALFORMED_PACKET, IPv4 header error, version is not IPv4 or header length field error.
X'04010002'	Attack, type=MALFORMED_PACKET, IPv4 header error, header length field or total length field error.

Table 26. Intrusion detection services probeids (continued)	
probeid	**description**
X'04010003'	Attack, type=MALFORMED_PACKET, IPv4 header error, total length field error.
X'04010004'	Attack, type=MALFORMED_PACKET, IPv4 header error, fragment offset field error.
X'04010005'	Attack, type=MALFORMED_PACKET, IPv4 header error, source IP address/destination IP address error.
X'04010006'	Attack, type=MALFORMED_PACKET, IPv4 header error, source IP address/destination IP address error.
X'04010007'	Attack, type=MALFORMED_PACKET, IPv4 header error, header length field or total length field error.
X'04010008'	Attack, type=MALFORMED_PACKET, IP header/TCP header error, source and destination IP addresses and source and destination ports error.
X'04010009'	Attack, type=MALFORMED_PACKET, IPv4 header error, header length field error.
X'0401000A'	Attack, type=MALFORMED_PACKET, IPv4 header error, destination address error, protocol is TCP and destination IP address is a multicast address.
X'0401000B'	Attack, type=MALFORMED_PACKET, IPv4 packet length error, packet does not include the entire TCP header.
X'0401000C'	Attack, type=MALFORMED_PACKET, IPv4 packet length error, packet does not include the entire UDP header.
X'0401000D'	Attack, type=MALFORMED_PACKET, IPv4 ICMP header error, option type not valid.
X'0401000E'	Attack, type=MALFORMED_PACKET, IPv4 header error, source IP address error, address is the unspecified address.
X'0401000F'	Attack, type=MALFORMED_PACKET, IPv4 header error, source IP address error, address is the loopback address, but the packet was not received on the loopback interface.
X'04010010'	Attack, type=MALFORMED_PACKET, IPv4 header error, destination IP address error, address is the loopback address, but the packet was not received on the loopback interface.
X'04010011'	Attack, type=MALFORMED_PACKET, IPv4 header error, length is too short for non-final fragment.
X'0401001E'	Attack, type=MALFORMED_PACKET, IPv6 header error, source or destination IP address error, address is the loopback address, but the packet was received over an external interface.
X'0401001F'	Attack, type=MALFORMED_PACKET, IPv6 packet length error, packet does not include the entire TCP header.
X'04010020'	Attack, type=MALFORMED_PACKET, IPv6 packet length error, packet does not include the entire UDP header.
X'04010021'	Attack, type=MALFORMED_PACKET, IPv6 header error, destination IP address error, address is the loopback address, but the packet was not received on the loopback interface.
X'04010023'	Attack, type=MALFORMED_PACKET, IPv6 header error, source IP address/destination IP address error.
X'04010024'	Attack, type=MALFORMED_PACKET, IPv6 header error, total length field error.
X'04010025'	Attack, type=MALFORMED_PACKET, IPv6 header error, version is not IPv6.

Table 26. Intrusion detection services probeids (continued)	
probeid	**description**
X'04010026'	Attack, type=MALFORMED_PACKET, IPv6 header error, source or destination IP address error, address is an IPv4-mapped IPv6 address.
X'04010027'	Attack, type=MALFORMED_PACKET, IPv6 header error, source IP address error, address is the loopback address, but the packet was not received on the loopback interface.
X'04010028'	Attack, type=MALFORMED_PACKET, IPv6 header error, destination IP address error, protocol is TCP and destination IP address is a multicast address.
X'04010029'	Attack, type=MALFORMED_PACKET, IPv6 header error, source IP address error, address is the unspecified address.
X'0401002A'	Attack, type=MALFORMED_PACKET, IPv6 header error, destination IP address error, IP address is a link-local address, but the packet was not received over the interface to which the link-local address is assigned.
X'04010032'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, inner IPv6 header not valid when previous header is an IPv6 header.
X'04010033'	Attack, type=MALFORMED_PACKET, IPv6 ICMP option error, bad length specified for an option in the packet.
X'04010034'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, fragment header is duplicated or in a location that is not valid.
X'04010035'	Attack, type=MALFORMED_PACKET, IPv6 fragment header error, fragment header included and payload length is zero.
X'04010036'	Attack, type=MALFORMED_PACKET, IPv6 fragment header error, fragment is not last and payload length is not multiple of 8.
X'04010037'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, hop-by-hop options header is in a location that is not valid.
X'04010038'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, multiple ICMPv6 error headers encountered.
X'04010039'	Attack, type=MALFORMED_PACKET, IPv6 ICMP option error, source link-layer address option in a Neighbor Discovery packet specifies the unspecified address.
X'0401003A'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, an inner IPv6 header was found in a packet that is using transport mode IP Security.
X'0401003B'	Attack, type=MALFORMED_PACKET, IPv6 ICMP option error, Neighbor Solicitation message with a source IP address that is not the unspecified address and a destination IP address that is a multicast address, source link-layer address option is missing.
X'0401003C'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, an inner IPv6 header was not found in a packet that is using tunnel mode IP Security.
X'0401003D'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, next header value of No Next Header is in a location that is not valid.
X'0401003E'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, unexpected IPv6 header encountered.
X'0401003F'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, bad length specified for an option in a hop-by-hop options header or a destination options header
X'04010040'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, IPv6 length field exceeds remaining packet length.

Table 26. Intrusion detection services probeids (continued)	
probeid	**description**
X'04010041'	Attack, type=MALFORMED_PACKET, IPv6 routing header error, routing header contains a multicast address.
X'04010042'	Attack, type=MALFORMED_PACKET, IPv6 extension header parsing error, destination IP address is a multicast address and packet contains a routing header.
X'04010043'	Attack, type=MALFORMED_PACKET, IPv6 routing header error, length value is not valid.
X'04010044'	Attack, type=MALFORMED_PACKET, IPv6 routing header error, segments left value is not valid.
X'04010045'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, header sub-type not valid.
X'04010046'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, duplicate header encountered.
X'04010047'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, security label in header did not match security label from first IP header.
X'04010048'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, header length not valid.
X'04010049'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, header encountered in a reassembled packet or following a routing header.
X'0401004A'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, security label missing from the first IP header.
X'0401004B'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, RACF domain not valid.
X'0401004C'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, tag length not valid.
X'0401004D'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, tag name missing.
X'0401004E'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, security label missing.
X'0401004F'	Attack, type=MALFORMED_PACKET, error in proprietary packet tagging header for multilevel security, tag type not valid.
X'04010050'	Attack, type=MALFORMED_PACKET, IPv6 ICMP header error, router advertisement message with source IP address that is not a link-local address, hop limit that is not 255, or ICMP code that is not 0.
X'04010051'	Attack, type=MALFORMED_PACKET, IPv6 ICMP header error, neighbor solicitation message with source IP address that is the unspecified address and destination IP address that is not a solicited-node multicast address, target IP address that is a multicast address, hop limit that is not 255, or ICMP code that is not 0.
X'04010052'	Attack, type=MALFORMED_PACKET, IPv6 ICMP header error, neighbor advertisement message with destination IP address that is a multicast address and indication that it was solicited, target IP address that is a multicast address, hop limit that is not 255, or ICMP code that is not 0.

Table 26. Intrusion detection services probeids (continued)

probeid	description
X'04010053'	Attack, type=MALFORMED_PACKET, IPv6 ICMP header error, redirect message with source IP address that is not a link-local address, destination IP address that is a multicast address, target IP address that is not a link-local address and is not the destination IP address, hop limit that is not 255, target IP address that is a local address, or ICMP code that is not 0.
X'04010054'	Attack, type=MALFORMED_PACKET, IPv6 ICMP header error, multicast listener discovery (MLD) query message with source IP address that is not a link-local address, destination IP address that is not a multicast address, or hop limit that is not 1.
X'04010055'	Attack, type=MALFORMED_PACKET, IPv6 ICMP header error, multicast listener discovery (MLD) report message with source IP address that is not a link-local address, destination IP address that is not a multicast address, or hop limit that is not 1.
X'04010056'	Attack, type=MALFORMED_PACKET, IPv6 ICMP header error, multicast listener discovery (MLD) reduction message with source IP address that is not a link-local address, destination IP address that is not a multicast address, or hop limit that is not 1.
X'0401FFF0'	Attack, type=MALFORMED_PACKET, Log records suppressed for malformed packet attacks.
X'04020001'	Attack, type=OUTBOUND_RAW, IP protocol restricted.
X'04020002'	Attack, type=OUTBOUND_RAW, application built IP header, source IP address not in home list.
X'04020003'	Attack, type=OUTBOUND_RAW, application built IP header, datagram fragmented.
X'04020004'	Attack, type=OUTBOUND_RAW, application built IP header, ICMP reply datagram.
X'04020005'	Attack, type=OUTBOUND_RAW, application built IP header, IP protocol restricted.
X'04020006'	Attack, type=OUTBOUND_RAW, ICMP reply datagram.
X'0402FFF0'	Attack, type=OUTBOUND_RAW, Log records suppressed for outbound raw attacks.
X'04030001'	Attack, type=IP_FRAGMENT, datagram fragmented within the first 88 bytes.
X'04030002'	Attack, type=IP_FRAGMENT, IPv4 fragment overlay, previously received fragments and data in overlay area is not the same.
X'04030003'	Attack, type=IP_FRAGMENT, IPv4 fragment received, fragment indicates length of original datagram is different from length indicated by previously received fragments.
X'04030004'	Attack, type=IP_FRAGMENT, IPv4 fragment received, fragment indicates length of original datagram is different from length indicated by previously received fragments.
X'04030011'	Attack, type=IP_FRAGMENT, IPv6 fragment overlay, previously received fragments and data in overlay area is not the same.
X'04030012'	Attack, type=IP_FRAGMENT, IPv6 fragment received, fragment indicates length of original datagram is different from length indicated by previously received fragments.
X'04030013'	Attack, type=IP_FRAGMENT, IPv6 fragment received, fragment indicates length of original datagram is different from length indicated by previously received fragments.
X'0403FFF0'	Attack, type=IP_FRAGMENT, Log records suppressed for IP fragment attacks.
X'04040001'	Attack, type=ICMP_REDIRECT, ICMP Redirect datagram.
X'0404FFF0'	Attack, type=ICMP_REDIRECT, Log records suppressed for ICMP Redirect attacks.
X'04050001'	Attack, type=RESTRICTED_IP_OPTIONS, datagram contains a restricted IP option.

Table 26. Intrusion detection services probeids (continued)	
probeid	**description**
X'0405FFF0'	Attack, type=RESTRICTED_IP_OPTIONS, Log records suppressed for restricted IP option attacks.
X'04060001'	Attack, type=RESTRICTED_IP_PROTOCOL, IP protocol restricted.
X'0406FFF0'	Attack, type=RESTRICTED_IP_PROTOCOL, Log records suppressed for restricted IP protocol attacks.
X'04070001'	Attack, type=FLOOD, Synflood end detected.
X'04070002'	Attack, type=FLOOD, Syn received during Synflood.
X'04070003'	Attack, type=FLOOD, Synflood end detected.
X'04070004'	Attack, type=FLOOD, Synflood end detected.
X'04070005'	Attack, type=FLOOD, Synflood end detected.
X'04070006'	Attack, type=FLOOD, Synflood end detected.
X'04070007'	Attack, type=FLOOD, Synflood end detected.
X'04070008'	Attack, type=FLOOD, Accept queue expanded.
X'04070009'	Attack, type=FLOOD, Synflood start detected.
X'04070010'	Attack, type=FLOOD, Interface Flood start detected.
X'04070011'	Attack, type=FLOOD, Interface Flood continuing. Written every five minutes while an interface flood lasts.
X'04070012'	Attack, type=FLOOD, Interface flood ended due to interface stopped.
X'04070013'	Attack, type=FLOOD, Interface flood ended due to FLOOD policy no longer active.
X'04070014'	Attack, type=FLOOD, Interface Flood Ended. Interface flood criteria no longer exceeded.
X'04070015'	Attack, type=FLOOD, Interface Flood Detection disabled for the interface due to storage constraints.
X'04070016'	Attack, type=FLOOD, Interface Flood data tracking temporarily suspended due to storage constraints.
X'04070017'	Attack, type=FLOOD, Synflood end detected.
X'04070101'	Attack, type=FLOOD, Interface Flood. Discard due to bad media header.
X'04070102'	Attack, type=FLOOD, Interface Flood. Discard due to unpacking problem.
X'04070103'	Attack, type=FLOOD, Interface Flood. Discard due to storage problem.
X'04070104'	Attack, type=FLOOD, Interface Flood. Discard due to bad checksum.
X'04070105'	Attack, type=FLOOD, Interface Flood. Discard due to malformed packet.
X'04070106'	Attack, type=FLOOD, Interface Flood. Discard due to destination.
X'04070107'	Attack, type=FLOOD, Interface Flood. Discard due to IDS policy.
X'04070108'	Attack, type=FLOOD, Interface Flood. Discard due to QoS policy.
X'04070109'	Attack, type=FLOOD, Interface Flood. Discard due to policy other than IDS or QoS policy.
X'0407010A'	Attack, type=FLOOD, Interface Flood. Discard due to netaccess, multilevel security, or OSM access checks.

Table 26. Intrusion detection services probeids (continued)	
probeid	**description**
X'0407010B'	Attack, type=FLOOD, Interface Flood. Discard due to forwarding error.
X'0407010C'	Attack, type=FLOOD, Interface Flood. Discard due to IP Security checks.
X'0407010D'	Attack, type=FLOOD, Interface Flood. Discard due to state problem.
X'0407010E'	Attack, type=FLOOD, Interface Flood. Discard due to problem not otherwise defined.
X'0407010F'	Attack, type=FLOOD, Interface Flood. Discard due to miscellaneous connection errors.
X'04070110'	Attack, type=FLOOD, Interface Flood. Discard due to queue limits exceeded.
X'04070111'	Attack, type=FLOOD, Interface Flood. Discard due to AT-TLS policy.
X'0407FFF0'	Attack, type=FLOOD, Log records suppressed for flood attacks.
X'04080001'	Attack, type=PERPETUAL_ECHO, UDP perpetual echo detected.
X'04080002'	Attack, type=PERPETUAL_ECHO, UDP perpetual echo detected.
X'04080003'	Attack, type=PERPETUAL_ECHO, UDP perpetual echo detected, port unreachable.
X'0408FFF0'	Attack, type=PERPETUAL_ECHO, Log records suppressed for perpetual echo attacks.
X'04090001'	Attack, type=DATA_HIDING, packet contains non-zero padding in the IP options.
X'04090002'	Attack, type=DATA_HIDING, packet contains non-zero padding in the IPv6 Destination Options header.
X'04090003'	Attack, type=DATA_HIDING, packet contains non-zero padding in the IPv6 hop-by-hop options header.
X'04090004'	Attack, type=DATA_HIDING, destination IP address in ICMP error packet does not match source IP address in embedded packet.
X'0409FFF0'	Attack, type=DATA_HIDING, Log records suppressed for data hiding attacks.
X'040A0001'	Attack, type=TCP_QUEUE_SIZE, TCP receive queue constrained.
X'040A0002'	Attack, type=TCP_QUEUE_SIZE, TCP receive queue unconstrained.
X'040A0003'	Attack, type=TCP_QUEUE_SIZE, Connection reset due to TCP receive queue constrained.
X'040A0004'	Attack, type=TCP_QUEUE_SIZE, TCP send queue constrained.
X'040A0005'	Attack, type=TCP_QUEUE_SIZE, TCP send queue unconstrained.
X'040A0006'	Attack, type=TCP_QUEUE_SIZE, Connection reset due to TCP send queue constrained.
X'040A0007'	Attack, type=TCP_QUEUE_SIZE, TCP out-of-order queue constrained.
X'040A0008'	Attack, type=TCP_QUEUE_SIZE, TCP out-of-order queue unconstrained.
X'040A0009'	Attack, type=TCP_QUEUE_SIZE, Connection reset due to TCP out-of-order queue constrained.
X'040AFFF0'	Attack, type=TCP_QUEUE_SIZE, Log records suppressed for TCP queue size attacks.
X'040B0001'	Attack, type=GLOBAL_TCP_STALL, global TCP stall attack started.
X'040B0002'	Attack, type=GLOBAL_TCP_STALL, global TCP stall attack ended.
X'040B0003'	Attack, type=GLOBAL_TCP_STALL, global TCP stall attack ended because IDS Global TCP Stall policy no longer in effect.
X'040B0004'	Attack, type=GLOBAL_TCP_STALL, Connection reset due to global TCP stall attack.

Table 26. Intrusion detection services probeids (continued)	
probeid	**description**
X'040B0005'	Attack, type=GLOBAL_TCP_STALL, Connection would have been reset due to global TCP stall attack.
X'040BFFF0'	Attack, type=GLOBAL_TCP_STALL, Log records suppressed for Global TCP stall attacks.
X'040C0001'	Attack, type=OUTBOUND_RAW_IPV6, IP protocol restricted.
X'040C0002'	Attack, type=OUTBOUND_RAW_IPV6, ICMPv6 reply datagram.
X'040C0003'	Attack, type=OUTBOUND_RAW_IPV6, ICMPv6 Router Advertisement, Router Solicitation, Neighbor Advertisement, or Neighbor Solicitation datagram.
X'040C0004'	Attack, type=OUTBOUND_RAW_IPV6, ICMPv6 MLD Listener Query, MLD Listener Report, MLD Listener Reduction, or MLDv2 Listener Report datagram.
X'040CFFF0'	Attack, type=OUTBOUND_RAW_IPV6, Log records suppressed for IPv6 outbound raw attacks.
X'040D0001'	Attack, type=RESTRICTED_IPV6_NEXT_HDR, packet contains a restricted IPv6 next header value.
X'040DFFF0'	Attack, type=RESTRICTED_IPV6_NEXT_HDR, Log records suppressed for restricted IPv6 next header attacks.
X'040E0001'	Attack, type=RESTRICTED_IPV6_DST_OPTIONS, packet contains an IPv6 Destination Options extension header with a restricted option.
X'040EFFF0'	Attack, type=RESTRICTED_IPV6_DST_OPTIONS, Log records suppressed for restricted IPv6 destination option attacks.
X'040F0001'	Attack, type=RESTRICTED_IPV6_HOP_OPTIONS, packet contains an IPv6 Hop-by-Hop Options extension header with a restricted option.
X'040FFFF0'	Attack, type=RESTRICTED_IPV6_HOP_OPTIONS, Log records suppressed for restricted IPv6 hop-by-hop option attacks.
X'04100001'	Attack, type=EE_LDLC_CHECK, an EE packet, other than data and a test probe, received on a destination port other than the signalling port.
X'0410FFF0''	Attack, type=EE_LDLC_CHECK, Log records suppressed for attacks detected by EE LDLC checking.
X'04110001'	Attack, type=EE_MALFORMED_PACKET, a malformed packet was received on an EE port.
X'0411FFF0'	Attack, type=EE_MALFORMED_PACKET, Log records suppressed for attacks detected by EE malformed packet checking.
X'04120001'	Attack, type=EE_PORT_CHECK, a packet was received with an incorrect source port address for EE.
X'0412FFF0'	Attack, type=EE_PORT_CHECK, Log records suppressed for attacks detected by EE port checking.
X'04130001'	Attack, type=EE_XID_FLOOD, A non-responsive XID was logged.
X'04130002'	Attack, type=EE_XID_FLOOD, An XID flood start was detected.
X'04130003'	Attack, type=EE_XID_FLOOD, An XID flood end was detected.
X'0413FFF0'	Attack, type=EE_XID_FLOOD, Log records suppressed for EE XID flood attacks.

Chapter 19. Resolver return and reason codes

This topic information describes the return codes and the reason codes generated by the resolver.

Resolver return codes

This section describes the return codes returned by the resolver. Table 27 on page 789 describes the return codes for the getaddrinfo, getnameinfo, and freeaddrinfo resolver APIs. Return codes for the gethostbyname and gethostbyaddr resolver APIs are described in Table 28 on page 790.

Table 27. Resolver return codes for getaddrinfo, getnameinfo, and freeaddrinfo

Code	Name	Description	Programmer's response
1	EAI_NONAME	This can be one of the following situations: • The name does not resolve for the supplied parameters. • Neither hostname nor servicename were supplied.	Check the validity of function parameters, TCPIP.DATA values, DNS definitions, or local host file (for example, etc.ipnodes). Also, ensure that your TCP/IP stack is active.
2	EAI_AGAIN	The name could not be resolved at this time. Future attempts might succeed.	The function is not able to complete, but the condition might not last a long time. Another call attempt can be tried almost immediately. Also, ensure that your resolver is active.
3	EAI_FAIL	A non-recoverable error occurred when attempting to resolve the name.	Check the validity of function parameters and TCPIP.DATA values.
4	EAI_OVERFLOW	The output buffer for the host name or service name was too small.	Increase the size of the buffer. Use the associated reason code to determine which buffer was too small.
5	EAI_FAMILY	The address family was not recognized or the address length was invalid length for the specified family.	Check the validity of function parameters.
6	EAI_MEMORY	There was a memory allocation failure when trying to allocate storage.	Increase the user storage allocation for this job.
7	EAI_BADFLAGS	The flags parameter had an invalid value.	Check the validity of function parameters.
8	EAI_SERVICE	The service passed was not recognized for the specified socket type.	Check the validity of function parameters, and local services file (for example, /etc/services or etc.services)
9	EAI_SOCKTYPE	The intended socket type was not recognized.	Check the validity of function parameters.

© Copyright IBM Corp. 2000, 2021

Table 28. Resolver return codes for gethostbyname and gethostbyaddr			
Code	**Name**	**Description**	**Programmer's response**
1	HOST_NOT_ FOUND	The name specified is unknown, the address domain specified is not supported, or the address length specified is not valid.	Check the validity of function parameters, TCPIP.DATA values, and DNS definitions.
2	TRY_AGAIN	Temporary error; information not currently accessible.	The function is not able to complete, but the condition might not last a long time. Another call attempt can be tried almost immediately. Also, ensure that your resolver is active.
3	NO_RECOVERY	Unrecoverable error occurred.	Check the validity of function parameters and TCPIP.DATA values.
4	NO_DATA	There is no data of the requested type for the host name.	Check the validity of function parameters, TCPIP.DATA values, and DNS definitions.

Resolver reason codes

This section describes the resolver reason codes, listing them by decimal and hexadecimal value.

The hexadecimal reason code is made up of 4 bytes in the following format:

```
cccc rrrr
```

Reason code qualifier	Reason code value
cccc	rrrr

- *cccc* is the reason code qualifier. If *cccc* is in the range of X'7800' through X'78FF', the reason code is defined by the Resolver.
- *rrrr* is the reason code value. If *cccc* is in the range of X'7800' through X'78FF', the value is described in the following table. If *cccc* is outside of that range, it is not a Resolver reason code. Those reason codes are described in the z/OS UNIX System Services Messages and Codes.

Table 29. Resolver reason codes			
Decimal value	**Hexadecimal value**	**Reason code**	**Description**
0—4095	0000—0FFF	defined by UNIX System Services	See the z/OS UNIX System Services Messages and Codes.
4096	1000	RSN_NotUp	Resolver service is not available.
4097	1001	RSN_BadEnv	Resolver service does not support SRB mode.
4098	1002	RSN_NoSpace	Resolver service output buffer is too small.
4099	1003	RSN_BadValue	Resolver service input parameter value is not valid.
4100	1004	RSN_NotFound	Resolver service did not find the specified host name.
4101	1005	RSN_BadAnswer	Resolver service received a bad answer from the nameserver, or did not receive an answer from the nameserver.

Table 29. Resolver reason codes (continued)

Decimal value	Hexadecimal value	Reason code	Description
4102	1006	RSN_BadParm	Resolver service was unable to access an input or output parameter.
4103	1007	RSN_BadSrv	Resolver service requested is not supported.
4104	1008	RSN_NoStorage	Resolver service received a negative answer from the nameserver, or did not receive an answer from the nameserver.
4105	1009	RSN_EintrRcv	Resolver service was interrupted by a signal.
4106	100A	EZB_RSN_NameIsAddr	An IP address was passed a name that was expected.
4107	100B	EZB_RSN_NoOmvsAuth	Service invoker not authorized to use USS.
4108	100C	EZB_RSN_NoLatches	Unable to obtain GRS latch set.
4109	100D	EZB_RSN_NameLenErr	Incorrect name length passed.
4110	100E	EZB_RSN_NestedAPI	Resolver service detected that there is still an outstanding resolver API request in the same task.
4111	100F	EZB_RSN_ServLenErr	Resolver service detected incorrect service name length.
4112	1010	EZB_RSN_SocketLenErr	Resolver service detected incorrect socket length.
4113	1011	EZB_RSN_NoData	No data was passed to Resolver service.
4114	1012	EZB_RSN_ServiceNotFound	Resolver service detected service name is not found.
4115	1013	EZB_RSN_PortNotFound	Resolver service detected port number is not found.
4116	1014	EZB_RSN_NoSocket	Resolver service detected there is no socket.
4117	1015	EZB_RSN_BadAddrinfo	Resolver service detected there is a bad input addrinfo.
4118	1016	EZB_RSN_InvalidSeq	Resolver service detected that freeaddrinfo was invoked without any addrinfos having been created.
4119	1017	EZB_RSN_BadProtocol	Resolver service detected invalid protocol.
4120	1018	EZB_RSN_SockLookup	Resolver service detected invalid socktype.
4121	1019	EZB_RSN_InvalidHostname	The host name input on a Getaddrinfo call contained only scope information.
4122	101A	EZB_RSN_ScopeNotPermitted	Scope information was specified on a Getaddrinfo call that has incompatible search options.
4123	101B	EZB_RSN_UnresolvedScope	The scope information specified on a Getaddrinfo or Getnameinfo call did not resolve to valid interface information on this system.

Table 29. Resolver reason codes (continued)

Decimal value	Hexadecimal value	Reason code	Description
4124	101C	EZB_RSN_HostnameBuffer	The buffer passed on the Getnameinfo call was too small for the resolved host name information; the application does not support receiving truncated information as a response.
4125	101D	EZB_RSN_ServicenameBuffer	The buffer passed on the Getnameinfo call was too small for the resolved service name information; the application does not support receiving truncated information as a response.
4216	101E	EZB_RSN_InvalidScopeValue	Scope information was specified on a Getaddrinfo call but was not in the correct format.

Chapter 20. TCP/IP Discard reason codes

The OSAENTA command collects packets from the Open System Adapter (OSA) that might have been discarded. The PKTTRACE command collects packets from TCPIP that might have been discarded. Each command returns a specific nonzero reason code when the packet has been discarded by their respective functions.

OSA-Express uses the discard reason codes from 1 to 4095 (see the *OSA network traffic analyzer (OSAENTA) discard codes* information in Open Systems Adapter-Express Customer's Guide and Reference for more information about OSA discard reason codes), and TCP/IP uses the discard codes from 4096 to 20479. Packets discarded by the Interface (IF) and IP layer use the discard reason codes from 4096 to 8191; packets discarded in the TCP protocol layer use the discard reason codes from 8192 to 12287; packets discarded in the UDP protocol layer use the discard reason codes from 12288 to 16383; packets discarded in the RAW protocol layer use the discard reason codes from 16384 to 20479.

Table 30 on page 793 describes the packet trace discard reason codes for the IP protocol. Table 31 on page 800 describes the packet trace discard reason codes for the TCP protocol. Table 32 on page 803 describes the packet trace discard reason codes for the UDP protocol. Table 33 on page 805 describes the packet trace discard reason codes for the RAW protocol.

Table 30. Packet trace discard reason codes for the IP protocol

Hex	Decimal	PKTTRACE IP DISCARD CODE VALUES	Meaning
1000	4096	IP_NO_INTERF	No interface was found for the packet because the interface had been deleted.
1001	4097	IP_NOT_ACTIVE	The interface is not active.
1002	4098	IP_MAL_VER	The IP version field is not IPv4 or IPv6.
1003	4099	IP_MAL_IPHL	The IP header length is too short.
1004	4100	IP_MAL_IPLEN	The IP header length is longer than the packet.
1005	4101	IP_MAL_DATA	The packet data is incomplete as sent.
1006	4102	IP_BAD_CKSUM	The IP header checksum is not valid.
1007	4103	IP_BAD_IPLEN	Packet is not long enough for a protocol header.
1008	4104	IP_OPT_IDS	The IP option is restricted by IDS Policy.
1009	4105	IP_OPT_SECLBL	A security label is not allowed.
100A	4106	IP_OPT_NATT	Network address translation option is not allowed.
100B	4107	IP_OPT_FWD	The packet cannot be forwarded.
100C	4108	IP_IDS_PROTO	The IP protocol is disallowed by IDS policy.
100D	4109	IP_MAP_ADDR	IPv6-mapped addresses are not supported.
100E	4110	IP_SRC_ADDR	The source address is a loopback address.
100F	4111	IP_SRC_HOST	The source address is a host address.
1010	4112	IP_DST_ADDR	The destination address is a loopback address or broadcast address.

© Copyright IBM Corp. 2000, 2021

Table 30. Packet trace discard reason codes for the IP protocol (continued)			
Hex	**Decimal**	**PKTTRACE IP DISCARD CODE VALUES**	**Meaning**
1011	4113	IP_NO_MULTI	There is no multicast listener.
1012	4114	IP_MAC_BRDCST	The MAC broadcast packet not accepted.
1013	4115	IP_XCF_NONEWCONN	Discard SYN packet to allow a new XCF connection to be established.
1014	4116	IP_XCF_SYNACK	The new DVIPA connection has not been received.
1015	4117	IP_XCF_TONOROUTE	No route is available during takeover or takeback.
1016	4118	IP_XCF_SERVDOWN	No server was found with a listen active.
1017	4119	IP_XCF_NODXCF	Dynamic XCF is not active.
1018	4120	IP_XCF_NOTDVIPA	This is not a DVIPA or it is DVIPA that is not active.
1019	4121	IP_XCF_NODXCFRTE	Dynamic XCF has no active routes.
101A	4122	IP_XCF_NOCONN	The connection request was received out of order.
101B	4123	IP_XCF_NODVIPA	The stack is not currently joined to the sysplex.
101C	4124	IP_XCF_NOROUTE	There is not a route available for the packet.
101D	4125	IP_XCF_NODEST	There is not an available target stack for the packet.
101E	4126	IP_XCF_NOTREADY	The target destination stack was not ready.
101F	4127	IP_XCF_ERROR	An error occurred in XCF routing.
1020	4128	IP_XCF_NOAFFIN	A fixed affinity structure could not be created.
1021	4129	IP_XCF_NOSTOR	No storage was available for a new connection.
1022	4130	IP_XCF_AFFTO	The backup DVIPA has not yet connected. A takeover is in progress.
1023	4131	IP_XCF_NOSECLBL	An MLS security label is missing.
1024	4132	IP_XCF_BADSECLBL	An unknown MLS security label was found.
1025	4133	IP_XCF_MISMATCH	There is a connection integrity problem with the target DVIPA.
1026	4134	IP_XCF_NOVIPARTE	No VIPAROUTE was found.
1027	4135	IP_XCF_NOACTRTE	No active VIPAROUTE was found.
1028	4136	IP_XCF_NOTTAKE	There is no route available for takeover or takeback.
1029	4137	IP_XCF_SYNCH	An encapsulated packet was received before a new connection could be established.

Table 30. Packet trace discard reason codes for the IP protocol (continued)

Hex	Decimal	PKTTRACE IP DISCARD CODE VALUES	Meaning
102A	4138	IP_XCF_TERM	XCF is ending.
102B	4139	IP_GRE_ADDR	The address family in the GRE SRE is not IPv4.
102C	4140	IP_GRE_PROTO	The protocol in the GRE header is not IPv4.
102D	4141	IP_GRE_SIZE	The GRE header in the buffer is incomplete.
102F	4143	IP_BAD_TCP_LEN	The packet length does not include the TCP header.
1030	4144	IP_BAD_UDP_LEN	The packet length does not include the UDP header.
1031	4145	IP_RSMTO	There was a reassembly timeout.
1032	4146	IP_CASA_NOACCEPT	The CASA packet was not accepted.
1033	4147	IP_FW_NOACCEPT	The firewall did not accept the packet.
1034	4148	IP_FW_KEEPALIVE	The NAT ESP keeplive packet was discarded.
1035	4149	IP_FW_MISMATCH	There was a mismatch with the firewall tunnel.
1036	4150	IP_FW_REJECT	The packet was rejected by the firewall.
1037	4151	IP_FW_NOSTOR	Storage was unavailable for the firewall function.
1038	4152	IP_FW_REJECTRC	The packet was rejected by the firewall. A bad return code was seen.
1039	4153	IP_INCOMP_ADDR	The IPv6 interface address is not complete.
103A	4154	IP_LNKLCL_ADDR	The destination address is not on the same physical network.
103B	4155	IP_HDR_OPT	The IP packet header options were bad or could not be updated.
103C	4156	IP_FWD_TTL	The IP packet timed out when the TTL field became 0.
103D	4157	IP_FWD_LCLBCAST	The IP packet cannot be forwarded to a local broadcast interface.
103E	4158	IP_FWD_NOSTOR	There was not enough storage to create the outbound packet.
103F	4159	IP_FWD_NOMSG	There was not enough storage available to copy the outbound packet.
1041	4161	IP_FRAG_SHORT	The fragment is too short to be processed.
1042	4162	IP_FRAG_DEATH	The fragment ending offset is greater than the maximum allowable packet size of a Ping of Death packet
1043	4163	IP_FRAG_ATTACK	The packet fragment appears to be an attack.

Table 30. Packet trace discard reason codes for the IP protocol (continued)

Hex	Decimal	PKTTRACE IP DISCARD CODE VALUES	Meaning
1044	4164	IP_BAD_ADDR	The destination address of the packet is not correct.
1045	4165	IP_MAL_ADDR	The destination address is the same as the source address.
1046	4166	IP_TCP_ADDR	The destination address for a TCP packet is incorrect.
1047	4167	IP_NO_FWD	The packet cannot be forwarded.
1048	4168	IP_BADMEDIA	The media header was incorrect.
1049	4169	IP_NODATA	There was not enough data in the packet for an IP header.
104A	4170	IP_NODEVICE	An active device interface was not found for the packet.
104B	4171	IP_NOTRDY_INTF	The interface was not ready for traffic.
104C	4172	IP_BAD_IPV6	Invalid inner IPv6 header where the previous IP header was an IPv6 header.
104D	4173	IP_NOT_IPV6	Invalid inner IPv6 header where the previous IP header was not an IPv6 header.
104E	4174	IP_HOPOPTS	The HOPOPTS extension header is misplaced.
104F	4175	IP_MISS_SLLA_OPT	The source link address is missing from a neighbor solicit ICMPv6 packet.
1050	4176	IP_NONE	The extension header was misplaced.
1051	4177	IP_PULLUP	The interface was not ready for traffic.
1052	4178	IP_ICMP_ERR	There are multiple ICMPV6 error headers.
1053	4179	IP_OPTS_DISCARD	The option type in a HOPOPTS or DESTOPTS extension header is not supported.
1054	4180	IP_OPTS_ERROR	The option type in a IP header, HOPOPTS extension header, or DESTOPTS extension header is not supported.
1055	4181	IP_OPTS_TYPE	The option type in a HOPOPTS or DESTOPTS extension header is not supported.
1056	4182	IP_ROUTING_LEN	The length of a routine extension header was incorrect.
1057	4183	IP_ROUTING_SEGLEFT	The **segments left** value in the routing extension header was incorrect.
1058	4184	IP_ROUTING_ADDR	An unsupported address was found in the routing extension header.
1059	4185	IP_ROUTING_SEGADDR	The address in the routing extension header was not a valid address.

Table 30. Packet trace discard reason codes for the IP protocol (continued)

Hex	Decimal	PKTTRACE IP DISCARD CODE VALUES	Meaning
105A	4186	IP_ROUTING_SEGTTL	The TTL value became 0 while the routing extension header was being processed.
105B	4187	IP_ROUTING_HDR	A routing extension header was misplaced in the packet.
105C	4188	IP_FRAG_MF0	The payload length of fragment was not a multiple of 8 bytes.
105D	4189	IP_FRAG_BAD	The fragment extension header is duplicated or out of place.
105E	4190	IP_ROUTING_TYPE	An unknown routing type extension header was found.
105F	4191	IP_ESP	The ESP extension header is misplaced.
1060	4192	IP_AH	The AH extension header is misplaced.
1061	4193	IP_SRC_LINK_ADDR	The source link address was not valid.
1062	4194	IP_BAD_OPT_LEN	The ICMPV6 option length was bad.
1065	4197	IP_FRAG_DATA	The fragment contains no data.
1066	4198	IP_OPTS_LEN	The option length in HOPOPTS or DSTOPTS extension header is is not correct.
1067	4199	IP_BAD_ICMP	An unknown ICMP type or code value was found.
1068	4200	IP_SECLBL_NO	A security extension header was present but is not supported.
1069	4201	IP_SECLBL_DUP	A duplicate security extension header was found.
106A	4202	IP_SECLBL_LEN	The length of the security extension header was incorrect.
106B	4203	IP_SECLBL_TAGNAME	The set name is missing from the security extension header.
106C	4204	IP_SECLBL_TAGTYPE	The tag type was incorrect in the security extension header.
106D	4205	IP_SECLBL_TAGLEN	The tag length was incorrect in the security extension header.
106E	4206	IP_SECLBL_TAGDOM	The RACF domain was missing from the security extension header.
106F	4207	IP_SECLBL_TAGSEC	The security label was missing from the security extension header.
1070	4208	IP_SECLBL_NOLBL	The security label was missing from the first IP header.
1071	4209	IP_SECLBL_IPHDR	The security label did not match the security label from the first IP header security extension.

Table 30. Packet trace discard reason codes for the IP protocol (continued)

Hex	Decimal	PKTTRACE IP DISCARD CODE VALUES	Meaning
1072	4210	IP_SECLBL_NFOUND	The label from the security extension header was not found.
1073	4211	IP_SECLBL_BADTYPE	The **type** field from the security extension header was not recognized.
1074	4212	IP_ROUTFWD_TYPE	The routing extension header for the packet that was forwarded contains a unknown type value.
1075	4213	IP_ROUTFWD_DEST	The forwared packet is being routed to an incorrect address.
1076	4214	IP_ROUTFWD_LEN	The routing extension header for a forwarded packet contains a bad **length** value.
1077	4215	IP_ROUTFWD_SEGLEFT	The routing extension header for a forwarded packet contains a bad **segments left** value.
1078	4216	IP_ROUTFWD_ADDR	The routing extension header for a forwarded packet contains a bad forwarding address.
1079	4217	IP_INNER_IPHDR	An unexpected inner IP header was found.
107A	4218	IP_NOIPHDR	The expected inner IP header was not found.
107B	4219	IP_QUICKDISCARD	A null packet was discarded.
107C	4220	IP_DUP_RST_4_DVIPA	A duplicate RST was passed to the distributor and should be silently discarded.
107D	4221	IP_XCF_THRT	Our Sysplex Throttle limit has been met, we should silently discard hoping resources have been freed.
107E	4222	IP_BAD_NTA_FRAME	A bad OSAENTA frame was found.
107F	4223	IP_IDS_NEXTHDR	The IPv6 next header is disallowed by IDS policy.
1080	4224	IP_IDS_HOPOPTS	The IPv6 hop-by-hop option is disallowed by IDS policy.
1081	4225	IP_IDS_DSTOPTS	The IPv6 destination option is disallowed by IDS policy.
1082	4226	IP_ND_RA	An IPv6 Router Advertisement has one of the following errors: • source IP address is not a link-local address • hop limit is not 255 • ICMP code is not 0

Table 30. Packet trace discard reason codes for the IP protocol (continued)

Hex	Decimal	PKTTRACE IP DISCARD CODE VALUES	Meaning
1083	4227	IP_ND_NS	An IPv6 Neighbor Solicitation has one of the following errors: • source IP address is the unspecified address and destination IP address is not a solicited-node multicast address • target IP address is a multicast address • hop limit is not 255 • ICMP code is not 0
1084	4228	IP_ND_NA	An IPv6 Neighbor Advertisement has one of the following errors: • destination IP address is a multicast address and advertisement indicates it was solicited • target IP address is a multicast address • hop limit is not 255 • ICMP code is not 0
1085	4229	IP_ND_REDIRECT	An ICMPv6 Redirect has one of the following errors: • source IP address is not a link-local address • destination IP address is a multicast address • target IP address is not a link-local address and is not the destination IP address • hop limit is not 255 • target IP address is a local address • ICMP code is not 0
1086	4230	IP_MLD_QUERY	An MLD Query message has one of the following errors: • source IP address is not a link-local address • destination IP address is not a multicast address • hop limit is not 1
1087	4231	IP_MLD_REPORT	An MLD Report message has one of the following errors: • source IP address is not a link-local address • destination IP address is not a multicast address • hop limit is not 1

Table 30. Packet trace discard reason codes for the IP protocol (continued)

Hex	Decimal	PKTTRACE IP DISCARD CODE VALUES	Meaning
1088	4232	IP_MLD_REDUCTION	An MLD Reduction message has one of the following errors: • source IP address is not a link-local address • destination IP address is not a multicast address • hop limit is not 1
1089	4233	IP_TRANS_NO_RCV	The transport is not receiving.
108A	4234	IP_FRAG_CANCEL	Fragmentation reassembly was cancelled.
108B	4235	IP_FRAG_DUP	Fragment is a duplicate of a previously received fragment.
108C	4236	IP_FRAG_LIMIT	Fragmentation reassembly not started - reassembly limit exceeded.
108D	4237	IP_FRAG_NOSTOR	No storage for fragmentation reassembly.
108E	4238	IP_ICMP_BAD_CKSUM	The ICMP header checksum is bad.
108F	4239	IP_QOS_POLICY	Packet denied by QoS policy.
1090	4240	IP_ICMP_NOSTOR	There was no storage for ICMP processing.
1091	4241	IP_IGNORE_REDIRECT	ICMP Redirect ignored due to configuration or IDS policy.
1092	4242	IP_BAD_ICMP_LEN	The ICMP packet length does not include the ICMP header or does not include the required length of data.
1093	4243	IP_OPT_NATT_EXT	Extended network address translation option is not allowed.
1094	4244	IP_IDS_DATAHIDE_IPOPT	Non-zero bytes in IP option padding are disallowed by IDS policy.
1095	4245	IP_IDS_DATAHIDE_DSTOPT	Non-zero bytes in destination option header padding are disallowed by IDS policy.
1096	4246	IP_IDS_DATAHIDE_HOPOPT	Non-zero bytes in hop-by-hop option header padding are disallowed by IDS policy.
1097	4247	IP_IDS_DATAHIDE_ICMPERR	ICMP error message with destination that does not match source of embedded packet is disallowed by IDS policy.
1098-1FFF	4248-8191	N/A	Codes reserved for future use.

Table 31. Packet Trace Discard reason codes for the TCP Protocol

Hex	Decimal	PKTTRACE TCP DISCARD CODE VALUES	Meaning
2000	8192	TCP_ALREADY_KLOSED	The session is already closed or about to be opened or for a listen.

Table 31. Packet Trace Discard reason codes for the TCP Protocol (continued)

Hex	Decimal	PKTTRACE TCP DISCARD CODE VALUES	Meaning
2001	8193	TCP_DATA_TOO_SHORT	Not all the data is present in the packet.
2002	8194	TCP_BAD_CHECKSUM	The TCP header checksum is incorrect.
2003	8195	TCP_OUTSIDE_WINDOW	The segment falls outside of the current window sequence space.
2004	8196	TCP_RECEIVED_RESET	A reset has been received.
2005	8197	TCP_MISSING_ACK	Once connected the ACK flag should always be set.
2006	8198	TCP_RECEIVED_LASTACK	The stream was closed when this last ACK was processed.
2007	8199	TCP_TCB_HEADLESS	There is no longer a connection with the socket.
2008	8200	TCP_NO_LISTENER	There is no listen active to accept the SYN request.
2009	8201	TCP_ACK_TOO_HIGH	The ACK sequence number is greater than the next sequence number to be sent.
200A	8202	TCP_CONNECT_RESET	A reset was received during the three-way handshake.
200B	8203	TCP_CONNECT_FAIL	The ACK sequence number was not correct for the SYN.
200C	8204	TCP_FRCA_RESET	AFPA reset the FRCA connection.
200D	8205	TCP_FRCA_FAIL	The connection was aborted by AFPA.
200E	8206	TCP_ALREADY_ TIMEWAIT	The connection has been closed and TCP is waiting for the ACK FIN.
200F	8207	TCP_OLD_TIMESTAMP	The timestamp on a TCP packet is older than the timestamp on a packet that was previously processed from the sender.
2010	8208	TCP_FRR_REACH_ THRESH	Entering fast retransmit recovery.
2011	8209	TCP_FRR_EXCEED_ THRESH	Discarding input for fast retransmit recovery; the window was exceeded.
2012	8210	TCP_FIREWALL_DENY	The IPSEC instances do not match.
2013	8211	TCP_INTRUSION_DENY	IDS has denied the connection as a result of a flood attack.
2014	8212	TCP_SECLABEL_PRESENT	An MLS security label was present but the socket did not expect one.
2015	8213	TCP_SECLABEL_NOT_ PRESENT	An MLS security label was not present but the socket expected one.
2016	8214	TCP_SECLABELS_NOT_ EQUIV	The MLS security labels were unacceptable to RACF.

Table 31. Packet Trace Discard reason codes for the TCP Protocol (continued)

Hex	Decimal	PKTTRACE TCP DISCARD CODE VALUES	Meaning
2017	8215	TCP_BAD_ACKNUM	The ACK sequence number is greater than the greatest sequence number that was sent.
2018	8216	TCP_TOO_SMALL	The size of the IP and TCP headers is longer than the packet.
2019	8217	TCP_BADHDR	The size of the TCP header is smaller than the minimum length allowed.
201A	8218	TCP_SYN_NOPORT	The local port connection was not found. The SYN packet was ignored.
201B	8219	TCP_SYN_NOTFOUND2	The local port connection was not listening. The SYN packet was ignored.
201C	8220	TCP_SYN_DUPTCP	A TCP session for this connection has already been established. The SYN packet was ignored.
201D	8221	TCP_SYN_RESET	A TCP packet was received with the RST flag set. The RST packet was ignored.
201E	8222	TCP_SYN_DUPSYN	A duplicate SYN packet has been received with a matching sequence number and the current TCP is in SYNCHRCV state. The SYN packet was ignored.
2020	8224	TCP_SYN_PORT	SHAREPORT or SHAREPORTWLM has been specified and a bind to a specific remote port has been performed. The incoming SYN was not from that remote port. The SYN packet was ignored.
2021	8225	TCP_SYN_BACKLOG0	The backlog count was set to 0. No sessions can be queued. The SYN packet was ignored.
2022	8226	TCP_SYN_BACKLOGS	No new sessions can be queued because the backlog count would be exceeded. The SYN packet was ignored.
2023	8227	TCP_SYN_BACKLOGE	The backlog count would be exceeded as a result of a possible SYN flood attack. The backlog queue cannot be extended. The SYN packet was ignored.
2024	8228	TCP_SYN_BACKLOGN	During a SYN flood attack, the backlog queue could not be expanded as the result of a storage shortage. The SYN packet was ignored.
2025	8229	TCP_SYN_BACKLOGR	During a SYN flood attack a backlog queue entry could not be randomally released. The SYN packet was ignored.
2026	8230	TCP_SYN_ROUTE	A route back to the remote host could not be determined. The SYN packet was ignored.

Table 31. Packet Trace Discard reason codes for the TCP Protocol (continued)

Hex	Decimal	PKTTRACE TCP DISCARD CODE VALUES	Meaning
2027	8231	TCP_SYN_STORAGE	No storage was available to define the connection control blocks. The SYN packet was ignored.
2028	8232	TCP_SYN_STATE	The SYN packet arrived for a connection to a port that was not in LISTEN state. The SYN packet was ignored.
2029	8233	TCP_SYN_ADDCONN	An unknown condition has occurred when attempting to set up the connection. The SYN packet was ignored.
202A	8234	TCP_SYN_POLICY	A policy was defined that required that the connection be reset. A RESET was sent back to the host.
202B	8235	TCP_SYN_MALFORMED	The IP addresses and port numbers are the same. The SYN packet was ignored.
202C	8236	TCP_SYN_NETACCESS	The netaccess RACF definitions required that the connection be reset. A RESET was sent back to the host.
202D	8237	TCP_SYN_FIREWALL	The netaccess RACF definitions required that the connection be reset. A RESET was sent back to the host.
202E	8238	TCP_SYN_DUPCONN	A SYN request has been received that requests a connection that has already been established. The SYN packet was ignored.
202F	8239	TCP_ATTLS_DROP	A packet was dropped because the secure data flow closed due to a SSL close notify and the remote partner did not accept the SSL close notify from ATTLS.
2030	8240	TCP_SYN_OSMERROR	OSM connections must only come from link local addresses. A RESET was sent back to the host.
2031	8241	TCP_NO_CONN	A packet was dropped because its TCP connection was not found.
2032	8242	DRC_TCP_ATTLS_ERR	A packet was dropped because AT-TLS reset the connection due to an error.
2033-2FFF	8243-12287	N/A	Codes reserved for future use

Table 32. Packet Trace Discard reason codes for the UDP Protocol

Hex	Decimal	PKTTRACE UDP DISCARD CODE VALUES	Meaning
3000	12288	UDP_IDS_UDPTR	Packet discarded by IDS UDP TR due to port constraint.
3001	12289	UDP_IDS_PERPECHO	IDS detected that the packet would cause a perpetual echo.

Table 32. Packet Trace Discard reason codes for the UDP Protocol (continued)

Hex	Decimal	PKTTRACE UDP DISCARD CODE VALUES	Meaning
3002	12290	UDP_EE_LDLCCHECK	Enterprise Extender packet received on wrong port
3003	12291	UDP_EE_PORTCHECK	Enterprise Extender packet detected with incorrect source port
3004	12292	UDP_EE_MALFORMED	Enterprise Extender received a malformed packet
3005	12293	N/A	Code reserved for future use.
3006	12294	UDP_NO_SOCKET	Datagram discarded because no UDP socket was found.
3007	12295	UDP_QOS_POLICY	Datagram denied by QoS policy.
3008	12296	UDP_FW_NOSTOR	Datagram discarded because there is not sufficient storage for IP Security checks.
3009	12297	UDP_FIREWALL_DENY	Datagram denied by IP Security checks.
300A	12298	UDP_BAD_LEN	Datagram is larger than receive buffer size.
300B	12299	UDP_NOT_CONN_ADDR	Datagram discarded because source IP address is not the address for the connected socket.
300C	12300	UDP_BAD_CKSUM	Datagram discarded due to bad UDP checksum.
300D	12301	UDP_STATE_PROB	Datagram discarded because UDP socket is in wrong state.
300E	12302	UDP_MALFORMED	Datagram discarded because it exceeds the maximum size allowed for a UDP datagram.
300F	12303	UDP_OTHER_POL	Datagram discarded because it exceeds the configured maximum size for a UDP datagram.
3010	12304	UDP_QUEUE_FULL	Datagram discarded because receive queue is full.
3011	12305	UDP_NETACCESS	Datagram denied by netaccess.
3012	12306	UDP_NOSTOR	Datagram discarded because there is not sufficient storage available to process the packet.
3013	12307	UDP_ROUTE_MISMATCH	ICMP datagram discarded because the destination IP address in the inner UDP packet did not match the route destination last used by this UDP socket.
3014	12308	UDP_ICMP_TIME	ICMP time exceeded or source quench packet discarded.
3015	12309	UDP_OSMACCESS	Datagram denied by OSM access.
3016 - 3FFF	12310 - 16383	N/A	Codes reserved for future use.

Table 33. Packet Trace Discard reason codes for the RAW Protocol

Hex	Decimal	PKTTRACE RAW DISCARD CODE VALUES	Meaning
4000	16384	RAW_IDS_OUTRAW	Packet discarded by IDS Attack Outbound Raw or Outbound Raw IPv6 checking.
4001	16385	RAW_NO_SOCKET	Datagram discarded because no raw socket was found.
4002	16386	RAW_QOS_POLICY	Datagram denied by QoS policy.
4003	16387	RAW_NOSTOR	There was no storage available to duplicate the datagram.
4004	16388	RAW_BAD_LEN	Datagram is larger than receive buffer size.
4005	16389	RAW_NOT_CONN_ADDR	Datagram discarded because source IP address is not the address for the connected socket.
4006	16390	RAW_QUEUE_FULL	Datagram discarded because receive queue is full.
4007	16391	RAW_NETACCESS	Datagram denied by netaccess.
4008	16392	RAW_MULTIPLE	Datagram denied for multiple reasons.
4009	16393	RAW_OSMACCESS	Datagram denied by OSM access.
400A - 4FFF	16394 - 20479	N/A	Codes reserved for future use.

Chapter 21. ENF event code 80 return and reason codes

This section describes the return codes and reason codes that the event notification facility (ENF) generates for the event code 80 processing.

Table 34. Return codes and reason codes for ENF event code 80 processing

Return Code	Reason code	Description	Programmer's Response
1	Return code from the STORAGE macro in hexadecimal format. For information about return codes, see "Return and reason codes" in z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO.	An error occurred obtaining storage in ECSA subpool 241.	Follow Steps for reviewing a storage problem in z/OS Communications Server: IP Diagnosis Guide to investigate the storage problem.
2	Return code from ENFREQ macro in hexadecimal format.	An error occurred generating the ENF system event.	Use the return code from the ENFREQ macro to determine the problem. If the problem cannot be solved, contact the IBM Support Center.
3	Return code from the RESMGR ADD macro in hexadecimal format. For information about return codes from the ADD function, see "Return codes from the ADD function" in z/OS MVS Programming: Authorized Assembler Services Reference LLA-SDU.	An error was returned by the RESMGR macro.	Follow the instructions in the return code description. If the problem cannot be solved, contact the IBM Support Center.
4	Reason code is in hexadecimal with the format *xxxxyyyy*. *xxxx* is the return code from the STORAGE macro. *yyyy* is the return code from the RESMGR ADD macro.	An error occurred obtaining storage in ECSA subpool 241 and an error was returned by the RESMGR macro.	Use the return codes from each macro to determine the problem. If the problem cannot be solved, contact the IBM Support Center.

© Copyright IBM Corp. 2000, 2021

Table 34. Return codes and reason codes for ENF event code 80 processing (continued)

Return Code	Reason code	Description	Programmer's Response
5	Reason code is in hexadecimal with the format *xxxxyyyy*. *xxxx* is the return code from the ENFREQ macro. *yyyy* is the return code from the RESMGR ADD macro.	An error occurred generating the ENF system event and an error was returned by the RESMGR macro.	Use the return codes from each macro to determine the problem. If the problem cannot be solved, contact the IBM Support Center.

Appendix A. Related protocol specifications

This appendix lists the related protocol specifications (RFCs) for TCP/IP. The Internet Protocol suite is still evolving through requests for comments (RFC). New protocols are being designed and implemented by researchers and are brought to the attention of the Internet community in the form of RFCs. Some of these protocols are so useful that they become recommended protocols. That is, all future implementations for TCP/IP are recommended to implement these particular functions or protocols. These become the *de facto* standards, on which the TCP/IP protocol suite is built.

RFCs are available at http://www.rfc-editor.org/rfc.html.

Draft RFCs that have been implemented in this and previous Communications Server releases are listed at the end of this topic.

Many features of TCP/IP Services are based on the following RFCs:

RFC
Title and Author

RFC 652
Telnet output carriage-return disposition option D. Crocker

RFC 653
Telnet output horizontal tabstops option D. Crocker

RFC 654
Telnet output horizontal tab disposition option D. Crocker

RFC 655
Telnet output formfeed disposition option D. Crocker

RFC 657
Telnet output vertical tab disposition option D. Crocker

RFC 658
Telnet output linefeed disposition D. Crocker

RFC 698
Telnet extended ASCII option T. Mock

RFC 726
Remote Controlled Transmission and Echoing Telnet option J. Postel, D. Crocker

RFC 727
Telnet logout option M.R. Crispin

RFC 732
Telnet Data Entry Terminal option J.D. Day

RFC 733
Standard for the format of ARPA network text messages D. Crocker, J. Vittal, K.T. Pogran, D.A. Henderson

RFC 734
SUPDUP Protocol M.R. Crispin

RFC 735
Revised Telnet byte macro option D. Crocker, R.H. Gumpertz

RFC 736
Telnet SUPDUP option M.R. Crispin

RFC 749
Telnet SUPDUP—Output option B. Greenberg

RFC 765
File Transfer Protocol specification J. Postel

© Copyright IBM Corp. 2000, 2021

RFC 768
User Datagram Protocol J. Postel

RFC 779
Telnet send-location option E. Killian

RFC 791
Internet Protocol J. Postel

RFC 792
Internet Control Message Protocol J. Postel

RFC 793
Transmission Control Protocol J. Postel

RFC 820
Assigned numbers J. Postel

RFC 823
DARPA Internet gateway R. Hinden, A. Sheltzer

RFC 826
Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware D. Plummer

RFC 854
Telnet Protocol Specification J. Postel, J. Reynolds

RFC 855
Telnet Option Specification J. Postel, J. Reynolds

RFC 856
Telnet Binary Transmission J. Postel, J. Reynolds

RFC 857
Telnet Echo Option J. Postel, J. Reynolds

RFC 858
Telnet Suppress Go Ahead Option J. Postel, J. Reynolds

RFC 859
Telnet Status Option J. Postel, J. Reynolds

RFC 860
Telnet Timing Mark Option J. Postel, J. Reynolds

RFC 861
Telnet Extended Options: List Option J. Postel, J. Reynolds

RFC 862
Echo Protocol J. Postel

RFC 863
Discard Protocol J. Postel

RFC 864
Character Generator Protocol J. Postel

RFC 865
Quote of the Day Protocol J. Postel

RFC 868
Time Protocol J. Postel, K. Harrenstien

RFC 877
Standard for the transmission of IP datagrams over public data networks J.T. Korb

RFC 883
Domain names: Implementation specification P.V. Mockapetris

RFC 884
Telnet terminal type option M. Solomon, E. Wimmers

RFC 885
Telnet end of record option J. Postel

RFC 894
Standard for the transmission of IP datagrams over Ethernet networks C. Hornig

RFC 896
Congestion control in IP/TCP internetworks J. Nagle

RFC 903
Reverse Address Resolution Protocol R. Finlayson, T. Mann, J. Mogul, M. Theimer

RFC 904
Exterior Gateway Protocol formal specification D. Mills

RFC 919
Broadcasting Internet Datagrams J. Mogul

RFC 922
Broadcasting Internet datagrams in the presence of subnets J. Mogul

RFC 927
TACACS user identification Telnet option B.A. Anderson

RFC 933
Output marking Telnet option S. Silverman

RFC 946
Telnet terminal location number option R. Nedved

RFC 950
Internet Standard Subnetting Procedure J. Mogul, J. Postel

RFC 952
DoD Internet host table specification K. Harrenstien, M. Stahl, E. Feinler

RFC 959
File Transfer Protocol J. Postel, J.K. Reynolds

RFC 961
Official ARPA-Internet protocols J.K. Reynolds, J. Postel

RFC 974
Mail routing and the domain system C. Partridge

RFC 1001
Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and methods NetBios Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, End-to-End Services Task Force

RFC 1002
Protocol Standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications NetBios Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, End-to-End Services Task Force

RFC 1006
ISO transport services on top of the TCP: Version 3 M.T. Rose, D.E. Cass

RFC 1009
Requirements for Internet gateways R. Braden, J. Postel

RFC 1011
Official Internet protocols J. Reynolds, J. Postel

RFC 1013
X Window System Protocol, version 11: Alpha update April 1987 R. Scheifler

RFC 1014
XDR: External Data Representation standard Sun Microsystems

RFC 1027
Using ARP to implement transparent subnet gateways S. Carl-Mitchell, J. Quarterman

RFC 1032
Domain administrators guide M. Stahl

RFC 1033
Domain administrators operations guide M. Lottor

RFC 1034
Domain names—concepts and facilities P.V. Mockapetris

RFC 1035
Domain names—implementation and specification P.V. Mockapetris

RFC 1038
Draft revised IP security option M. St. Johns

RFC 1041
Telnet 3270 regime option Y. Rekhter

RFC 1042
Standard for the transmission of IP datagrams over IEEE 802 networks J. Postel, J. Reynolds

RFC 1043
Telnet Data Entry Terminal option: DODIIS implementation A. Yasuda, T. Thompson

RFC 1044
Internet Protocol on Network System's HYPERchannel: Protocol specification K. Hardwick, J. Lekashman

RFC 1053
Telnet X.3 PAD option S. Levy, T. Jacobson

RFC 1055
Nonstandard for transmission of IP datagrams over serial lines: SLIP J. Romkey

RFC 1057
RPC: Remote Procedure Call Protocol Specification: Version 2 Sun Microsystems

RFC 1058
Routing Information Protocol C. Hedrick

RFC 1060
Assigned numbers J. Reynolds, J. Postel

RFC 1067
Simple Network Management Protocol J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin

RFC 1071
Computing the Internet checksum R.T. Braden, D.A. Borman, C. Partridge

RFC 1072
TCP extensions for long-delay paths V. Jacobson, R.T. Braden

RFC 1073
Telnet window size option D. Waitzman

RFC 1079
Telnet terminal speed option C. Hedrick

RFC 1085
ISO presentation services on top of TCP/IP based internets M.T. Rose

RFC 1091
Telnet terminal-type option J. VanBokkelen

RFC 1094
NFS: Network File System Protocol specification Sun Microsystems

RFC 1096
Telnet X display location option G. Marcy

RFC 1101
DNS encoding of network names and other types P. Mockapetris

RFC 1112
Host extensions for IP multicasting S.E. Deering

RFC 1113
Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures J. Linn

RFC 1118
Hitchhikers Guide to the Internet E. Krol

RFC 1122
Requirements for Internet Hosts—Communication Layers R. Braden, Ed.

RFC 1123
Requirements for Internet Hosts—Application and Support R. Braden, Ed.

RFC 1146
TCP alternate checksum options J. Zweig, C. Partridge

RFC 1155
Structure and identification of management information for TCP/IP-based internets M. Rose, K. McCloghrie

RFC 1156
Management Information Base for network management of TCP/IP-based internets K. McCloghrie, M. Rose

RFC 1157
Simple Network Management Protocol (SNMP) J. Case, M. Fedor, M. Schoffstall, J. Davin

RFC 1158
Management Information Base for network management of TCP/IP-based internets: MIB-II M. Rose

RFC 1166
Internet numbers S. Kirkpatrick, M.K. Stahl, M. Recker

RFC 1179
Line printer daemon protocol L. McLaughlin

RFC 1180
TCP/IP tutorial T. Socolofsky, C. Kale

RFC 1183
New DNS RR Definitions C.F. Everhart, L.A. Mamakos, R. Ullmann, P.V. Mockapetris

RFC 1184
Telnet Linemode Option D. Borman

RFC 1186
MD4 Message Digest Algorithm R.L. Rivest

RFC 1187
Bulk Table Retrieval with the SNMP M. Rose, K. McCloghrie, J. Davin

RFC 1188
Proposed Standard for the Transmission of IP Datagrams over FDDI Networks D. Katz

RFC 1190
Experimental Internet Stream Protocol: Version 2 (ST-II) C. Topolcic

RFC 1191
Path MTU discovery J. Mogul, S. Deering

RFC 1198
FYI on the X window system R. Scheifler

RFC 1207
FYI on Questions and Answers: Answers to commonly asked "experienced Internet user" questions G. Malkin, A. Marine, J. Reynolds

RFC 1208
Glossary of networking terms O. Jacobsen, D. Lynch

RFC 1213
Management Information Base for Network Management of TCP/IP-based internets: MIB-II K. McCloghrie, M.T. Rose

RFC 1215
Convention for defining traps for use with the SNMP M. Rose

RFC 1227
SNMP MUX protocol and MIB M.T. Rose

RFC 1228
SNMP-DPI: Simple Network Management Protocol Distributed Program Interface G. Carpenter, B. Wijnen

RFC 1229
Extensions to the generic-interface MIB K. McCloghrie

RFC 1230
IEEE 802.4 Token Bus MIB K. McCloghrie, R. Fox

RFC 1231
IEEE 802.5 Token Ring MIB K. McCloghrie, R. Fox, E. Decker

RFC 1236
IP to X.121 address mapping for DDN L. Morales, P. Hasse

RFC 1256
ICMP Router Discovery Messages S. Deering, Ed.

RFC 1267
Border Gateway Protocol 3 (BGP-3) K. Lougheed, Y. Rekhter

RFC 1268
Application of the Border Gateway Protocol in the Internet Y. Rekhter, P. Gross

RFC 1269
Definitions of Managed Objects for the Border Gateway Protocol: Version 3 S. Willis, J. Burruss

RFC 1270
SNMP Communications Services F. Kastenholz, ed.

RFC 1285
FDDI Management Information Base J. Case

RFC 1315
Management Information Base for Frame Relay DTEs C. Brown, F. Baker, C. Carvalho

RFC 1321
The MD5 Message-Digest Algorithm R. Rivest

RFC 1323
TCP Extensions for High Performance V. Jacobson, R. Braden, D. Borman

RFC 1325
FYI on Questions and Answers: Answers to Commonly Asked "New Internet User" Questions G. Malkin, A. Marine

RFC 1327
Mapping between X.400 (1988)/ISO 10021 and RFC 822 S. Hardcastle-Kille

RFC 1340
Assigned Numbers J. Reynolds, J. Postel

RFC 1344
Implications of MIME for Internet Mail Gateways N. Bornstein

RFC 1349
Type of Service in the Internet Protocol Suite P. Almquist

RFC 1351
SNMP Administrative Model J. Davin, J. Galvin, K. McCloghrie

RFC 1352
SNMP Security Protocols J. Galvin, K. McCloghrie, J. Davin

RFC 1353
Definitions of Managed Objects for Administration of SNMP Parties K. McCloghrie, J. Davin, J. Galvin

RFC 1354
IP Forwarding Table MIB F. Baker

RFC 1356
Multiprotocol Interconnect® on X.25 and ISDN in the Packet Mode A. Malis, D. Robinson, R. Ullmann

RFC 1358
Charter of the Internet Architecture Board (IAB) L. Chapin

RFC 1363
A Proposed Flow Specification C. Partridge

RFC 1368
Definition of Managed Objects for IEEE 802.3 Repeater Devices D. McMaster, K. McCloghrie

RFC 1372
Telnet Remote Flow Control Option C. L. Hedrick, D. Borman

RFC 1374
IP and ARP on HIPPI J. Renwick, A. Nicholson

RFC 1381
SNMP MIB Extension for X.25 LAPB D. Throop, F. Baker

RFC 1382
SNMP MIB Extension for the X.25 Packet Layer D. Throop

RFC 1387
RIP Version 2 Protocol Analysis G. Malkin

RFC 1388
RIP Version 2 Carrying Additional Information G. Malkin

RFC 1389
RIP Version 2 MIB Extensions G. Malkin, F. Baker

RFC 1390
Transmission of IP and ARP over FDDI Networks D. Katz

RFC 1393
Traceroute Using an IP Option G. Malkin

RFC 1398
Definitions of Managed Objects for the Ethernet-Like Interface Types F. Kastenholz

RFC 1408
Telnet Environment Option D. Borman, Ed.

RFC 1413
Identification Protocol M. St. Johns

RFC 1416
Telnet Authentication Option D. Borman, ed.

RFC 1420
SNMP over IPX S. Bostock

RFC 1428
Transition of Internet Mail from Just-Send-8 to 8bit-SMTP/MIME G. Vaudreuil

RFC 1442
Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1443
Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1445
Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2) J. Galvin, K. McCloghrie

RFC 1447
Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2) K. McCloghrie, J. Galvin

RFC 1448
Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1464
Using the Domain Name System to Store Arbitrary String Attributes R. Rosenbaum

RFC 1469
IP Multicast over Token-Ring Local Area Networks T. Pusateri

RFC 1483
Multiprotocol Encapsulation over ATM Adaptation Layer 5 Juha Heinanen

RFC 1514
Host Resources MIB P. Grillo, S. Waldbusser

RFC 1516
Definitions of Managed Objects for IEEE 802.3 Repeater Devices D. McMaster, K. McCloghrie

RFC 1521
MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies N. Borenstein, N. Freed

RFC 1535
A Security Problem and Proposed Correction With Widely Deployed DNS Software E. Gavron

RFC 1536
Common DNS Implementation Errors and Suggested Fixes A. Kumar, J. Postel, C. Neuman, P. Danzig, S. Miller

RFC 1537
Common DNS Data File Configuration Errors P. Beertema

RFC 1540
Internet Official Protocol Standards J. Postel

RFC 1571
Telnet Environment Option Interoperability Issues D. Borman

RFC 1572
Telnet Environment Option S. Alexander

RFC 1573
Evolution of the Interfaces Group of MIB-II K. McCloghrie, F. Kastenholz

RFC 1577
Classical IP and ARP over ATM M. Laubach

RFC 1583
OSPF Version 2 J. Moy

RFC 1591
Domain Name System Structure and Delegation J. Postel

RFC 1592
Simple Network Management Protocol Distributed Protocol Interface Version 2.0 B. Wijnen, G. Carpenter, K. Curran, A. Sehgal, G. Waters

RFC 1594
FYI on Questions and Answers— Answers to Commonly Asked "New Internet User" Questions A. Marine, J. Reynolds, G. Malkin

RFC 1644
T/TCP — TCP Extensions for Transactions Functional Specification R. Braden

RFC 1646
TN3270 Extensions for LUname and Printer Selection C. Graves, T. Butts, M. Angel

RFC 1647
TN3270 Enhancements B. Kelly

RFC 1652
SMTP Service Extension for 8bit-MIMEtransport J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker

RFC 1664
Using the Internet DNS to Distribute RFC1327 Mail Address Mapping Tables C. Allochio, A. Bonito, B. Cole, S. Giordano, R. Hagens

RFC 1693
An Extension to TCP: Partial Order Service T. Connolly, P. Amer, P. Conrad

RFC 1695
Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2 M. Ahmed, K. Tesink

RFC 1701
Generic Routing Encapsulation (GRE) S. Hanks, T. Li, D. Farinacci, P. Traina

RFC 1702
Generic Routing Encapsulation over IPv4 networks S. Hanks, T. Li, D. Farinacci, P. Traina

RFC 1706
DNS NSAP Resource Records B. Manning, R. Colella

RFC 1712
DNS Encoding of Geographical Location C. Farrell, M. Schulze, S. Pleitner D. Baldoni

RFC 1713
Tools for DNS debugging A. Romao

RFC 1723
RIP Version 2—Carrying Additional Information G. Malkin

RFC 1752
The Recommendation for the IP Next Generation Protocol S. Bradner, A. Mankin

RFC 1766
Tags for the Identification of Languages H. Alvestrand

RFC 1771
A Border Gateway Protocol 4 (BGP-4) Y. Rekhter, T. Li

RFC 1794
DNS Support for Load Balancing T. Brisco

RFC 1819
Internet Stream Protocol Version 2 (ST2) Protocol Specification—Version ST2+ L. Delgrossi, L. Berger Eds.

RFC 1826
IP Authentication Header R. Atkinson

RFC 1828
IP Authentication using Keyed MD5 P. Metzger, W. Simpson

RFC 1829
The ESP DES-CBC Transform P. Karn, P. Metzger, W. Simpson

RFC 1830
SMTP Service Extensions for Transmission of Large and Binary MIME Messages G. Vaudreuil

RFC 1831
RPC: Remote Procedure Call Protocol Specification Version 2 R. Srinivasan

RFC 1832
XDR: External Data Representation Standard R. Srinivasan

RFC 1833
Binding Protocols for ONC RPC Version 2 R. Srinivasan

RFC 1850
OSPF Version 2 Management Information Base F. Baker, R. Coltun

RFC 1854
SMTP Service Extension for Command Pipelining N. Freed

RFC 1869
SMTP Service Extensions J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker

RFC 1870
SMTP Service Extension for Message Size Declaration J. Klensin, N. Freed, K. Moore

RFC 1876
A Means for Expressing Location Information in the Domain Name System C. Davis, P. Vixie, T. Goodwin, I. Dickinson

RFC 1883
Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden

RFC 1884
IP Version 6 Addressing Architecture R. Hinden, S. Deering, Eds.

RFC 1886
DNS Extensions to support IP version 6 S. Thomson, C. Huitema

RFC 1888
OSI NSAPs and IPv6 J. Bound, B. Carpenter, D. Harrington, J. Houldsworth, A. Lloyd

RFC 1891
SMTP Service Extension for Delivery Status Notifications K. Moore

RFC 1892
The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages G. Vaudreuil

RFC 1894
*An Extensible Message Format for Delivery Status Notifications*K. Moore, G. Vaudreuil

RFC 1901
Introduction to Community-based SNMPv2 J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1902
Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1903
Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1904
Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1905
Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1906
Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1907
Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2) J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1908
Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1912
Common DNS Operational and Configuration Errors D. Barr

RFC 1918
Address Allocation for Private Internets Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear

RFC 1928
SOCKS Protocol Version 5 M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones

RFC 1930
Guidelines for creation, selection, and registration of an Autonomous System (AS) J. Hawkinson, T. Bates

RFC 1939
Post Office Protocol-Version 3 J. Myers, M. Rose

RFC 1981
Path MTU Discovery for IP version 6 J. McCann, S. Deering, J. Mogul

RFC 1982
Serial Number Arithmetic R. Elz, R. Bush

RFC 1985
SMTP Service Extension for Remote Message Queue Starting J. De Winter

RFC 1995
Incremental Zone Transfer in DNS M. Ohta

RFC 1996
A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY) P. Vixie

RFC 2010
Operational Criteria for Root Name Servers B. Manning, P. Vixie

RFC 2011
SNMPv2 Management Information Base for the Internet Protocol using SMIv2 K. McCloghrie, Ed.

RFC 2012
SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2 K. McCloghrie, Ed.

RFC 2013
SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2 K. McCloghrie, Ed.

RFC 2018
TCP Selective Acknowledgement Options M. Mathis, J. Mahdavi, S. Floyd, A. Romanow

RFC 2026
The Internet Standards Process — Revision 3 S. Bradner

RFC 2030
Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI D. Mills

RFC 2033
Local Mail Transfer Protocol J. Myers

RFC 2034
*SMTP Service Extension for Returning Enhanced Error Codes*N. Freed

RFC 2040
*The RC5, RC5–CBC, RC-5–CBC-Pad, and RC5–CTS Algorithms*R. Baldwin, R. Rivest

RFC 2045
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies N. Freed, N. Borenstein

RFC 2052
A DNS RR for specifying the location of services (DNS SRV) A. Gulbrandsen, P. Vixie

RFC 2065
Domain Name System Security Extensions D. Eastlake 3rd, C. Kaufman

RFC 2066
TELNET CHARSET Option R. Gellens

RFC 2080
RIPng for IPv6 G. Malkin, R. Minnear

RFC 2096
IP Forwarding Table MIB F. Baker

RFC 2104
HMAC: Keyed-Hashing for Message Authentication H. Krawczyk, M. Bellare, R. Canetti

RFC 2119
Keywords for use in RFCs to Indicate Requirement Levels S. Bradner

RFC 2133
Basic Socket Interface Extensions for IPv6 R. Gilligan, S. Thomson, J. Bound, W. Stevens

RFC 2136
Dynamic Updates in the Domain Name System (DNS UPDATE) P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound

RFC 2137
Secure Domain Name System Dynamic Update D. Eastlake 3rd

RFC 2163
Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM) C. Allocchio

RFC 2168
Resolution of Uniform Resource Identifiers using the Domain Name System R. Daniel, M. Mealling

RFC 2178
OSPF Version 2 J. Moy

RFC 2181
Clarifications to the DNS Specification R. Elz, R. Bush

RFC 2205
Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin

RFC 2210
The Use of RSVP with IETF Integrated Services J. Wroclawski

RFC 2211
Specification of the Controlled-Load Network Element Service J. Wroclawski

RFC 2212
Specification of Guaranteed Quality of Service S. Shenker, C. Partridge, R. Guerin

RFC 2215
General Characterization Parameters for Integrated Service Network Elements S. Shenker, J. Wroclawski

RFC 2217
Telnet Com Port Control Option G. Clarke

RFC 2219
Use of DNS Aliases for Network Services M. Hamilton, R. Wright

RFC 2228
FTP Security Extensions M. Horowitz, S. Lunt

RFC 2230
Key Exchange Delegation Record for the DNS R. Atkinson

RFC 2233
The Interfaces Group MIB using SMIv2 K. McCloghrie, F. Kastenholz

RFC 2240
A Legal Basis for Domain Name Allocation O. Vaughn

RFC 2246
The TLS Protocol Version 1.0 T. Dierks, C. Allen

RFC 2251
Lightweight Directory Access Protocol (v3) M. Wahl, T. Howes, S. Kille

RFC 2253
Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names M. Wahl, S. Kille, T. Howes

RFC 2254
The String Representation of LDAP Search Filters T. Howes

RFC 2261
An Architecture for Describing SNMP Management Frameworks D. Harrington, R. Presuhn, B. Wijnen

RFC 2262
Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 2271
An Architecture for Describing SNMP Management Frameworks D. Harrington, R. Presuhn, B. Wijnen

RFC 2273
SNMPv3 Applications D. Levi, P. Meyer, B. Stewartz

RFC 2274
User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) U. Blumenthal, B. Wijnen

RFC 2275
View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) B. Wijnen, R. Presuhn, K. McCloghrie

RFC 2279
UTF-8, a transformation format of ISO 10646 F. Yergeau

RFC 2292
Advanced Sockets API for IPv6 W. Stevens, M. Thomas

RFC 2308
Negative Caching of DNS Queries (DNS NCACHE) M. Andrews

RFC 2317
Classless IN-ADDR.ARPA delegation H. Eidnes, G. de Groot, P. Vixie

RFC 2320
Definitions of Managed Objects for Classical IP and ARP Over ATM Using SMIv2 (IPOA-MIB) M. Greene, J. Luciani, K. White, T. Kuo

RFC 2328
OSPF Version 2 J. Moy

RFC 2345
Domain Names and Company Name Retrieval J. Klensin, T. Wolf, G. Oglesby

RFC 2352
A Convention for Using Legal Names as Domain Names O. Vaughn

RFC 2355
TN3270 Enhancements B. Kelly

RFC 2358
Definitions of Managed Objects for the Ethernet-like Interface Types J. Flick, J. Johnson

RFC 2373
IP Version 6 Addressing Architecture R. Hinden, S. Deering

RFC 2374
An IPv6 Aggregatable Global Unicast Address Format R. Hinden, M. O'Dell, S. Deering

RFC 2375
IPv6 Multicast Address Assignments R. Hinden, S. Deering

RFC 2385
Protection of BGP Sessions via the TCP MD5 Signature Option A. Hefferman

RFC 2389
Feature negotiation mechanism for the File Transfer Protocol P. Hethmon, R. Elz

RFC 2401
Security Architecture for Internet Protocol S. Kent, R. Atkinson

RFC 2402
IP Authentication Header S. Kent, R. Atkinson

RFC 2403
The Use of HMAC-MD5–96 within ESP and AH C. Madson, R. Glenn

RFC 2404
The Use of HMAC-SHA–1–96 within ESP and AH C. Madson, R. Glenn

RFC 2405
The ESP DES-CBC Cipher Algorithm With Explicit IV C. Madson, N. Doraswamy

RFC 2406
IP Encapsulating Security Payload (ESP) S. Kent, R. Atkinson

RFC 2407
*The Internet IP Security Domain of Interpretation for ISAKMP*D. Piper

RFC 2408
Internet Security Association and Key Management Protocol (ISAKMP) D. Maughan, M. Schertler, M. Schneider, J. Turner

RFC 2409
The Internet Key Exchange (IKE) D. Harkins, D. Carrel

RFC 2410
The NULL Encryption Algorithm and Its Use With IPsec R. Glenn, S. Kent,

RFC 2428
FTP Extensions for IPv6 and NATs M. Allman, S. Ostermann, C. Metz

RFC 2445
Internet Calendaring and Scheduling Core Object Specification (iCalendar) F. Dawson, D. Stenerson

RFC 2459
Internet X.509 Public Key Infrastructure Certificate and CRL Profile R. Housley, W. Ford, W. Polk, D. Solo

RFC 2460
Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden

RFC 2461
Neighbor Discovery for IP Version 6 (IPv6) T. Narten, E. Nordmark, W. Simpson

RFC 2462
IPv6 Stateless Address Autoconfiguration S. Thomson, T. Narten

RFC 2463
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering

RFC 2464
Transmission of IPv6 Packets over Ethernet Networks M. Crawford

RFC 2466
Management Information Base for IP Version 6: ICMPv6 Group D. Haskin, S. Onishi

RFC 2476
Message Submission R. Gellens, J. Klensin

RFC 2487
SMTP Service Extension for Secure SMTP over TLS P. Hoffman

RFC 2505
Anti-Spam Recommendations for SMTP MTAs G. Lindberg

RFC 2523
Photuris: Extended Schemes and Attributes P. Karn, W. Simpson

RFC 2535
Domain Name System Security Extensions D. Eastlake 3rd

RFC 2538
Storing Certificates in the Domain Name System (DNS) D. Eastlake 3rd, O. Gudmundsson

RFC 2539
Storage of Diffie-Hellman Keys in the Domain Name System (DNS) D. Eastlake 3rd

RFC 2540
Detached Domain Name System (DNS) Information D. Eastlake 3rd

RFC 2554
SMTP Service Extension for Authentication J. Myers

RFC 2570
Introduction to Version 3 of the Internet-standard Network Management Framework J. Case, R. Mundy, D. Partain, B. Stewart

RFC 2571
An Architecture for Describing SNMP Management Frameworks B. Wijnen, D. Harrington, R. Presuhn

RFC 2572
Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 2573
SNMP Applications D. Levi, P. Meyer, B. Stewart

RFC 2574
User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) U. Blumenthal, B. Wijnen

RFC 2575
View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) B. Wijnen, R. Presuhn, K. McCloghrie

RFC 2576
Co-Existence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework R. Frye, D. Levi, S. Routhier, B. Wijnen

RFC 2578
Structure of Management Information Version 2 (SMIv2) K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2579
Textual Conventions for SMIv2 K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2580
Conformance Statements for SMIv2 K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2581
TCP Congestion Control M. Allman, V. Paxson, W. Stevens

RFC 2583
Guidelines for Next Hop Client (NHC) Developers R. Carlson, L. Winkler

RFC 2591
Definitions of Managed Objects for Scheduling Management Operations D. Levi, J. Schoenwaelder

RFC 2625
IP and ARP over Fibre Channel M. Rajagopal, R. Bhagwat, W. Rickard

RFC 2635
Don't SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam)* S. Hambridge, A. Lunde

RFC 2637
Point-to-Point Tunneling Protocol K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn

RFC 2640
Internationalization of the File Transfer Protocol B. Curtin

RFC 2665
Definitions of Managed Objects for the Ethernet-like Interface Types J. Flick, J. Johnson

RFC 2671
Extension Mechanisms for DNS (EDNS0) P. Vixie

RFC 2672
Non-Terminal DNS Name Redirection M. Crawford

RFC 2675
IPv6 Jumbograms D. Borman, S. Deering, R. Hinden

RFC 2710
Multicast Listener Discovery (MLD) for IPv6 S. Deering, W. Fenner, B. Haberman

RFC 2711
IPv6 Router Alert Option C. Partridge, A. Jackson

RFC 2740
OSPF for IPv6 R. Coltun, D. Ferguson, J. Moy

RFC 2753
A Framework for Policy-based Admission Control R. Yavatkar, D. Pendarakis, R. Guerin

RFC 2782
A DNS RR for specifying the location of services (DNS SRV) A. Gubrandsen, P. Vixix, L. Esibov

RFC 2821
Simple Mail Transfer Protocol J. Klensin, Ed.

RFC 2822
Internet Message Format P. Resnick, Ed.

RFC 2840
TELNET KERMIT OPTION J. Altman, F. da Cruz

RFC 2845
Secret Key Transaction Authentication for DNS (TSIG) P. Vixie, O. Gudmundsson, D. Eastlake 3rd, B. Wellington

RFC 2851
Textual Conventions for Internet Network Addresses M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 2852
Deliver By SMTP Service Extension D. Newman

RFC 2874
DNS Extensions to Support IPv6 Address Aggregation and Renumbering M. Crawford, C. Huitema

RFC 2915
The Naming Authority Pointer (NAPTR) DNS Resource Record M. Mealling, R. Daniel

RFC 2920
SMTP Service Extension for Command Pipelining N. Freed

RFC 2930
Secret Key Establishment for DNS (TKEY RR) D. Eastlake, 3rd

RFC 2941
Telnet Authentication Option T. Ts'o, ed., J. Altman

RFC 2942
Telnet Authentication: Kerberos Version 5 T. Ts'o

RFC 2946
Telnet Data Encryption Option T. Ts'o

RFC 2952
Telnet Encryption: DES 64 bit Cipher Feedback T. Ts'o

RFC 2953
Telnet Encryption: DES 64 bit Output Feedback T. Ts'o

RFC 2992
Analysis of an Equal-Cost Multi-Path Algorithm C. Hopps

RFC 3019
IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol B. Haberman, R. Worzella

RFC 3060
Policy Core Information Model—Version 1 Specification B. Moore, E. Ellesson, J. Strassner, A. Westerinen

RFC 3152
Delegation of IP6.ARPA R. Bush

RFC 3164
The BSD Syslog Protocol C. Lonvick

RFC 3207
SMTP Service Extension for Secure SMTP over Transport Layer Security P. Hoffman

RFC 3226
DNSSEC and IPv6 A6 aware server/resolver message size requirements O. Gudmundsson

RFC 3291
Textual Conventions for Internet Network Addresses M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 3363
Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain

RFC 3376
Internet Group Management Protocol, Version 3 B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan

RFC 3390
Increasing TCP's Initial Window M. Allman, S. Floyd, C. Partridge

RFC 3410
Introduction and Applicability Statements for Internet-Standard Management Framework J. Case, R. Mundy, D. Partain, B. Stewart

RFC 3411
An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks D. Harrington, R. Presuhn, B. Wijnen

RFC 3412
Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 3413
Simple Network Management Protocol (SNMP) Applications D. Levi, P. Meyer, B. Stewart

RFC 3414
User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) U. Blumenthal, B. Wijnen

RFC 3415
View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) B. Wijnen, R. Presuhn, K. McCloghrie

RFC 3416
Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3417
Transport Mappings for the Simple Network Management Protocol (SNMP) R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3418
Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3419
Textual Conventions for Transport Addresses M. Daniele, J. Schoenwaelder

RFC 3484
Default Address Selection for Internet Protocol version 6 (IPv6) R. Draves

RFC 3493
Basic Socket Interface Extensions for IPv6 R. Gilligan, S. Thomson, J. Bound, J. McCann, W. Stevens

RFC 3513
Internet Protocol Version 6 (IPv6) Addressing Architecture R. Hinden, S. Deering

RFC 3526
More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) T. Kivinen, M. Kojo

RFC 3542
Advanced Sockets Application Programming Interface (API) for IPv6 W. Richard Stevens, M. Thomas, E. Nordmark, T. Jinmei

RFC 3566
The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec S. Frankel, H. Herbert

RFC 3569
An Overview of Source-Specific Multicast (SSM) S. Bhattacharyya, Ed.

RFC 3584
Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework R. Frye, D. Levi, S. Routhier, B. Wijnen

RFC 3602
The AES-CBC Cipher Algorithm and Its Use with IPsec S. Frankel, R. Glenn, S. Kelly

RFC 3629
UTF-8, a transformation format of ISO 10646 R. Kermode, C. Vicisano

RFC 3658
Delegation Signer (DS) Resource Record (RR) O. Gudmundsson

RFC 3678
Socket Interface Extensions for Multicast Source Filters D. Thaler, B. Fenner, B. Quinn

RFC 3715
IPsec-Network Address Translation (NAT) Compatibility Requirements B. Aboba, W. Dixon

RFC 3810
Multicast Listener Discovery Version 2 (MLDv2) for IPv6 R. Vida, Ed., L. Costa, Ed.

RFC 3826
The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model U. Blumenthal, F. Maino, K McCloghrie.

RFC 3947
Negotiation of NAT-Traversal in the IKE T. Kivinen, B. Swander, A. Huttunen, V. Volpe

RFC 3948
UDP Encapsulation of IPsec ESP Packets A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg

RFC 4001
Textual Conventions for Internet Network Addresses M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 4007
IPv6 Scoped Address Architecture S. Deering, B. Haberman, T. Jinmei, E. Nordmark, B. Zill

RFC 4022
Management Information Base for the Transmission Control Protocol (TCP) R. Raghunarayan

RFC 4106
The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) J. Viega, D. McGrew

RFC 4109
Algorithms for Internet Key Exchange version 1 (IKEv1) P. Hoffman

RFC 4113
Management Information Base for the User Datagram Protocol (UDP) B. Fenner, J. Flick

RFC 4191
Default Router Preferences and More-Specific Routes R. Draves, D. Thaler

RFC 4217
Securing FTP with TLS P. Ford-Hutchinson

RFC 4292
IP Forwarding Table MIB B. Haberman

RFC 4293
Management Information Base for the Internet Protocol (IP) S. Routhier

RFC 4301
Security Architecture for the Internet Protocol S. Kent, K. Seo

RFC 4302
IP Authentication Header S. Kent

RFC 4303
IP Encapsulating Security Payload (ESP) S. Kent

RFC 4304
Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP) S. Kent

RFC 4307
Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2) J. Schiller

RFC 4308
Cryptographic Suites for IPsec P. Hoffman

RFC 4434
The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol P. Hoffman

RFC 4443
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering

RFC 4552
Authentication/Confidentiality for OSPFv3 M. Gupta, N. Melam

RFC 4678
Server/Application State Protocol v1 A. Bivens

RFC 4753
ECP Groups for IKE and IKEv2 D. Fu, J. Solinas

RFC 4754
IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA) D. Fu, J. Solinas

RFC 4809
Requirements for an IPsec Certificate Management Profile C. Bonatti, Ed., S. Turner, Ed., G. Lebovitz, Ed.

RFC 4835
Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) V. Manral

RFC 4862
IPv6 Stateless Address Autoconfiguration S. Thomson, T. Narten, T. Jinmei

RFC 4868
Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec S. Kelly, S. Frankel

RFC 4869
Suite B Cryptographic Suites for IPsec L. Law, J. Solinas

RFC 4941
Privacy Extensions for Stateless Address Autoconfiguration in IPv6 T. Narten, R. Draves, S. Krishnan

RFC 4945
The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX B. Korver

RFC 5014
IPv6 Socket API for Source Address Selection E. Nordmark, S. Chakrabarti, J. Laganier

RFC 5095
Deprecation of Type 0 Routing Headers in IPv6 J. Abley, P. Savola, G. Neville-Neil

RFC 5175
IPv6 Router Advertisement Flags Option B. Haberman, Ed., R. Hinden

RFC 5282
Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol D. Black, D. McGrew

RFC 5996
Internet Key Exchange Protocol Version 2 (IKEv2) C. Kaufman, P. Hoffman, Y. Nir, P. Eronen

RFC 7627
Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension K. Bhargavan, A. Delignat-Lavaud, A. Pironti, Inria Paris-Rocquencourt, A. Langley, M. Ray

RFC 8446
The Transport Layer Security (TLS) Protocol Version 1.3 E. Rescorla

Internet drafts

Internet drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Other groups can also distribute working documents as Internet drafts. You can see Internet drafts at http://www.ietf.org/ID.html.

Appendix B. Architectural specifications

This appendix lists documents that provide architectural specifications for the SNA Protocol.

The APPN Implementers' Workshop (AIW) architecture documentation includes the following architectural specifications for SNA APPN and HPR:

- APPN Architecture Reference (SG30-3422-04)
- APPN Branch Extender Architecture Reference Version 1.1
- APPN Dependent LU Requester Architecture Reference Version 1.5
- APPN Extended Border Node Architecture Reference Version 1.0
- APPN High Performance Routing Architecture Reference Version 4.0
- SNA Formats (GA27-3136-20)
- SNA Technical Overview (GC30-3073-04)

The following RFC also contains SNA architectural specifications:

- RFC 2353 *APPN/HPR in IP Networks APPN Implementers' Workshop Closed Pages Document*

RFCs are available at http://www.rfc-editor.org/rfc.html.

© Copyright IBM Corp. 2000, 2021

Appendix C. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you can view the information through the z/OS Internet Library website http://www.ibm.com/systems/z/os/zos/library/bkserv/ or IBM Documentation https://www.ibm.com/docs/en. If you continue to experience problems, send a message to Contact z/OS web page(www.ibm.com/systems/z/os/zos/webqs.html) or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. See z/OS TSO/E Primer, z/OS TSO/E User's Guide, and z/OS ISPF User's Guide Vol I for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

© Copyright IBM Corp. 2000, 2021

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the IBM Documentation. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation Site Counsel 2455 South Road Poughkeepsie, NY 12601-5400 USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

© Copyright IBM Corp. 2000, 2021

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com®/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Bibliography

This bibliography contains descriptions of the documents in the z/OS Communications Server library.

z/OS Communications Server documentation is available online at the z/OS Internet Library web page at http://www.ibm.com/systems/z/os/zos/library/bkserv/.

z/OS Communications Server library updates

Updates to documents are also available on RETAIN and in information APARs (info APARs). Go to https://www.ibm.com/mysupport to view information APARs.

- z/OS Communications Server V2R1 New Function APAR Summary
- z/OS Communications Server V2R2 New Function APAR Summary
- z/OS Communications Server V2R3 New Function APAR Summary
- z/OS Communications Server V2R4 New Function APAR Summary

z/OS Communications Server information

z/OS Communications Server product information is grouped by task in the following tables.

Planning

Title	Number	Description
z/OS Communications Server: New Function Summary	GC27-3664	This document is intended to help you plan for new IP or SNA functions, whether you are migrating from a previous version or installing z/OS for the first time. It summarizes what is new in the release and identifies the suggested and required modifications needed to use the enhanced functions.
z/OS Communications Server: IPv6 Network and Application Design Guide	SC27-3663	This document is a high-level introduction to IPv6. It describes concepts of z/OS Communications Server's support of IPv6, coexistence with IPv4, and migration issues.

Resource definition, configuration, and tuning

Title	Number	Description
z/OS Communications Server: IP Configuration Guide	SC27-3650	This document describes the major concepts involved in understanding and configuring an IP network. Familiarity with the z/OS operating system, IP protocols, z/OS UNIX System Services, and IBM Time Sharing Option (TSO) is recommended. Use this document with the z/OS Communications Server: IP Configuration Reference.

© Copyright IBM Corp. 2000, 2021

Title	Number	Description
z/OS Communications Server: IP Configuration Reference	SC27-3651	This document presents information for people who want to administer and maintain IP. Use this document with the z/OS Communications Server: IP Configuration Guide. The information in this document includes: • TCP/IP configuration data sets • Configuration statements • Translation tables • Protocol number and port assignments
z/OS Communications Server: SNA Network Implementation Guide	SC27-3672	This document presents the major concepts involved in implementing an SNA network. Use this document with the z/OS Communications Server: SNA Resource Definition Reference.
z/OS Communications Server: SNA Resource Definition Reference	SC27-3675	This document describes each SNA definition statement, start option, and macroinstruction for user tables. It also describes NCP definition statements that affect SNA. Use this document with the z/OS Communications Server: SNA Network Implementation Guide.
z/OS Communications Server: SNA Resource Definition Samples	SC27-3676	This document contains sample definitions to help you implement SNA functions in your networks, and includes sample major node definitions.
z/OS Communications Server: IP Network Print Facility	SC27-3658	This document is for systems programmers and network administrators who need to prepare their network to route SNA, JES2, or JES3 printer output to remote printers using TCP/IP Services.

Operation

Title	Number	Description
z/OS Communications Server: IP User's Guide and Commands	SC27-3662	This document describes how to use TCP/IP applications. It contains requests with which a user can log on to a remote host using Telnet, transfer data sets using FTP, send electronic mail, print on remote printers, and authenticate network users.
z/OS Communications Server: IP System Administrator's Commands	SC27-3661	This document describes the functions and commands helpful in configuring or monitoring your system. It contains system administrator's commands, such as TSO NETSTAT, PING, TRACERTE and their UNIX counterparts. It also includes TSO and MVS commands commonly used during the IP configuration process.
z/OS Communications Server: SNA Operation	SC27-3673	This document serves as a reference for programmers and operators requiring detailed information about specific operator commands.
z/OS Communications Server: Quick Reference	SC27-3665	This document contains essential information about SNA and IP commands.

Customization

Title	Number	Description
z/OS Communications Server: SNA Customization	SC27-3666	This document enables you to customize SNA, and includes the following information: • Communication network management (CNM) routing table • Logon-interpret routine requirements • Logon manager installation-wide exit routine for the CLU search exit • TSO/SNA installation-wide exit routines • SNA installation-wide exit routines

Writing application programs

Title	Number	Description
z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference	SC27-3660	This document describes the syntax and semantics of program source code necessary to write your own application programming interface (API) into TCP/IP. You can use this interface as the communication base for writing your own client or server application. You can also use this document to adapt your existing applications to communicate with each other using sockets over TCP/IP.
z/OS Communications Server: IP CICS Sockets Guide	SC27-3649	This document is for programmers who want to set up, write application programs for, and diagnose problems with the socket interface for CICS using z/OS TCP/IP.
z/OS Communications Server: IP IMS Sockets Guide	SC27-3653	This document is for programmers who want application programs that use the IMS TCP/IP application development services provided by the TCP/IP Services of IBM.
z/OS Communications Server: IP Programmer's Guide and Reference	SC27-3659	This document describes the syntax and semantics of a set of high-level application functions that you can use to program your own applications in a TCP/IP environment. These functions provide support for application facilities, such as user authentication, distributed databases, distributed processing, network management, and device sharing. Familiarity with the z/OS operating system, TCP/IP protocols, and IBM Time Sharing Option (TSO) is recommended.
z/OS Communications Server: SNA Programming	SC27-3674	This document describes how to use SNA macroinstructions to send data to and receive data from (1) a terminal in either the same or a different domain, or (2) another application program in either the same or a different domain.
z/OS Communications Server: SNA Programmer's LU 6.2 Guide	SC27-3669	This document describes how to use the SNA LU 6.2 application programming interface for host application programs. This document applies to programs that use only LU 6.2 sessions or that use LU 6.2 sessions along with other session types. (Only LU 6.2 sessions are covered in this document.)
z/OS Communications Server: SNA Programmer's LU 6.2 Reference	SC27-3670	This document provides reference material for the SNA LU 6.2 programming interface for host application programs.

Title	Number	Description
z/OS Communications Server: CSM Guide	SC27-3647	This document describes how applications use the communications storage manager.

Diagnosis

Title	Number	Description
z/OS Communications Server: IP Diagnosis Guide	GC27-3652	This document explains how to diagnose TCP/IP problems and how to determine whether a specific problem is in the TCP/IP product code. It explains how to gather information for and describe problems to the IBM Software Support Center.
z/OS Communications Server: ACF/TAP Trace Analysis Handbook	GC27-3645	This document explains how to gather the trace data that is collected and stored in the host processor. It also explains how to use the Advanced Communications Function/Trace Analysis Program (ACF/TAP) service aid to produce reports for analyzing the trace data information.
z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures and z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	GC27-3667 GC27-3668	These documents help you identify an SNA problem, classify it, and collect information about it before you call the IBM Support Center. The information collected includes traces, dumps, and other problem documentation.
z/OS Communications Server: SNA Data Areas Volume 1 and z/OS Communications Server: SNA Data Areas Volume 2	GC31-6852 GC31-6853	These documents describe SNA data areas and can be used to read an SNA dump. They are intended for IBM programming service representatives and customer personnel who are diagnosing problems with SNA.

Messages and codes

Title	Number	Description
z/OS Communications Server: SNA Messages	SC27-3671	This document describes the ELM, IKT, IST, IUT, IVT, and USS messages. Other information in this document includes: • Command and RU types in SNA messages • Node and ID types in SNA messages • Supplemental message-related information
z/OS Communications Server: IP Messages Volume 1 (EZA)	SC27-3654	This volume contains TCP/IP messages beginning with EZA.
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	SC27-3655	This volume contains TCP/IP messages beginning with EZB or EZD.
z/OS Communications Server: IP Messages Volume 3 (EZY)	SC27-3656	This volume contains TCP/IP messages beginning with EZY.
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	SC27-3657	This volume contains TCP/IP messages beginning with EZZ and SNM.
z/OS Communications Server: IP and SNA Codes	SC27-3648	This document describes codes and other information that appear in z/OS Communications Server messages.

Index

A

accessibility 831

C

Communications Server for z/OS, online information xxxix

D

disability 831
DNS, online information xl

I

IBM Software Support Center, contacting xxxvi
Information APARs xxxvii
Internet, finding z/OS information online xxxix

K

keyboard 831

L

license, patent, and copyright information 833

M

mainframe
    education xxxvii

P

prerequisite information xxxvii

R

RFC (request for comments)
    accessing online xxxix

S

shortcut keys 831
SNA protocol specifications 829
softcopy information xxxvii
summary of changes xliii

T

TCP/IP
    online information xxxix
    protocol specifications 809
Technotes xxxvii
trademark information 836

V

VTAM, online information xxxix

Z

z/OS Basic Skills Information Center xxxvii
z/OS, documentation library listing 837

Communicating your comments to IBM

Important: If your comment regards a technical question or problem, see instead “If you have a technical problem” on page 843.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM Documentation function
If your comment or question is about the IBMDocumentation functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Documentation Support at ibmdocs@us.ibm.com.

Feedback on the z/OS product documentation and content
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The title and order name of the document, and the version of z/OS Communications Server
- The section title of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

© Copyright IBM Corp. 2000, 2021

Product Number: 5650-ZOS

SC27-3648-40