

z/OS Communications Server



IP Migration

Version 1 Release 4

z/OS Communications Server



IP Migration

Version 1 Release 4

Note:

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 285.

Third Edition (September 2002)

This edition applies to Version 1 Release 4 of z/OS (5694-A01) and Version 1 Release 4 of z/OS.e (5655-G52) and to all subsequent releases and modifications until otherwise indicated in new editions.

Publications are not stocked at the address given below. If you want more IBM® publications, ask your IBM representative or write to the IBM branch office serving your locality.

A form for your comments is provided at the back of this document. If the form has been removed, you may address comments to:

IBM Corporation
Software Reengineering
Department G71A/ Bldg 503
Research Triangle Park, NC 27709-9990
U.S.A.

If you prefer to send comments electronically, use one of the following methods:

Fax (USA and Canada):

1-800-254-0206

Internet e-mail:

usib2hpd@vnet.ibm.com

World Wide Web:

<http://www.ibm.com/servers/eserver/zseries/zos/webqs.html>

IBMLink™:

CIBMORCF at RALVM17

IBM Mail Exchange:

tkinlaw@us.ibm.com

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1994, 2002. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	xiii
Tables	xv
About this document	xix
Who should use this document	xix
How this document is organized	xix
Where to find more information	xx
Where to find related information on the Internet	xx
Accessing z/OS licensed documents on the Internet	xxi
Using LookAt to look up message explanations.	xxii
How to contact IBM service	xxii
z/OS Communications Server information	xxiii
Summary of changes	xxxi
Chapter 1. Overview of z/OS Communications Server	1
What is z/OS Communications Server?	1
TCP/IP protocol stack	2
Connectivity and gateway functions	3
Network protocol layer	4
Transport layer	5
File systems	5
Application Programming Interfaces (APIs)	6
Applications	8
Application tables	9
Programming tools and libraries	15
TCP/IP packaging process	16
MVS data sets	16
HFS files	18
Encryption features	20
Chapter 2. Migration overview	23
Planning and migration checklist	27
Chapter 3. New and changed interfaces	29
Configuration files	29
TCPIP.DATA	31
PROFILE.TCPIP configuration file	31
SYS1.PARMLIB members	35
Operator commands	36
TSO commands	43
UNIX commands	49
Environment variables	58
Socket APIs	58
TCP/IP socket APIs enabled for IPv6 in z/OS CS V1R4	58
Socket APIs	59
IPCS subcommands	61
CTRACE COMP(SYSTCPDA) subcommand	61
CTRACE COMP(SYSTCPIS) subcommand	62
CTRACE COMP(SYSTCPRE) subcommand	62
INETSTAT subcommand	62
TCPIPES subcommand	63

Chapter 4. z/OS V1R4 Communications Server release summary	65
Migration considerations	65
Sysplex Distributor enhancements	66
Sysplex-wide Dynamic Source VIPAs for TCP connections	66
Sysplexports	67
Sysplex Wide Security Association (SWSA)	68
Access control for network and Fast Response Cache Accelerator (FRCA)	69
Network access control	69
Fast Response Cache Accelerator (FRCA) access control	70
Resolver enhancements	70
Restrictions	71
What this change affects	71
Migration procedures	71
Managed System Infrastructure (msys) for Setup enhancement	71
Restrictions	71
What this change affects	72
Migration procedures	72
OSA SNMP subagent support	72
Restrictions	72
What this change affects	72
Migration procedures	72
Event trace enhancements	72
Restrictions	72
What this change affects	72
Migration procedures	73
TCP/IP support for Simple Network Time Protocol (SNTP)	73
Restrictions	73
Dependencies	73
What this change affects	73
Migration procedures	73
Netstat enhancements	74
Restrictions	75
What this change affects	75
Migration procedures	75
Ping enhancements	75
Restrictions	75
What this change affects	76
Migration procedures	76
Traceroute enhancements	76
Restrictions	77
What this change affects	77
Migration procedures	77
New VTAM start options to adjust the QDIO or IQDIO storage	78
OSA Express storage for read processing	78
HiperSockets storage for read processing	78
Restrictions	78
What this change affects	79
Migration procedures	79
IPv6 support	79
Enabling IPv6 support	79
Configuration changes related to IPv6 support	80
IPv6 support for the resolver	82
IPv6 support for applications	83
IPv6 support for Netstat	84
IPv6 support for Ping	85
IPv6 support for Traceroute	85

	IPv6 support for IPv6 IPCS subcommands formatting	86
	IPv6 support for event trace enhancements	86
	IPv6 support for RAS packet trace and data trace	87
	IPv6 support for socket API commands	87
	Chapter 5. z/OS V1R3 Communications Server release summary	89
	Chapter 6. z/OS V1R2 Communications Server release summary	91
	Migration considerations	91
	Resolver enhancements	92
	Restrictions	93
	What this change affects	93
	Migration procedures.	93
	Intrusion Detection Services	95
	Restrictions	96
	Dependencies	96
	Incompatibilities	97
	What this change affects	97
	Migration procedures.	97
	Sysplex Distributor policy enhancements	98
	Incompatibilities	98
	What this change affects	98
	Migration procedures.	98
	Policy Agent enhancements.	100
	Restrictions.	100
	What this change affects	100
	Migration procedures	100
	OROUTED to OMPROUTE migration	102
	Restrictions.	103
	What this change affects	103
	Migration procedures	103
	OMPROUTE to allow RIP1 and RIP2 packets over the same interface	103
	Restrictions.	104
	What this change affects	104
	Migration procedures	104
	Replaceable static routes	104
	Restrictions.	104
	What this change affects	105
	Migration procedures	105
	OMPROUTE wildcard IP addressing enhancement	105
	Restrictions.	105
	What this change affects	105
	Migration procedures	106
	Additional RIP filter for OMPROUTE	106
	Restrictions.	106
	What this change affects	106
	Migration procedures	106
	OSPF MD5 authentication	106
	Restrictions.	106
	What this change affects	107
	Migration procedures	107
	Native Socket API TCP_NODELAY support	108
	Restrictions.	108
	What this change affects	108
	Migration procedures	108
	Netstat enhancements.	109

Netstat filter enhancements	109
Netstat performance counters	109
Restrict access to netstat commands	110
z/OS UNIX RSHD Kerberos support.	111
Restrictions	111
Incompatibilities	111
What this change affects	111
Migration procedures	111
Application-driven policy classification	112
Restrictions	112
What this change affects	112
Migration procedures	112
Virtual LAN priority tagging	112
Restrictions	113
Dependencies	113
What this change affects	113
Migration procedures	113
Packet trace enhancements.	113
Restrictions	113
What this change affects	113
Migration procedures	113
Fast connection reset for Sysplex Distributor	114
Restrictions	114
What this change affects	114
Migration procedures	114
HiperSockets	114
Restrictions	115
What this change affects	115
Migration procedures	115
Efficient routing using HiperSockets Accelerator	117
Restrictions	117
Dependencies	117
What this change affects	117
Migration procedures	117
Connection load balancing using Sysplex Distributor in a network with Cisco routers.	118
Restrictions	118
Dependencies	119
What this change affects	119
Migration procedures	119
CICS sockets listener enhancements	120
Restrictions	120
What this change affects	120
Migration procedures	120
SMF recording enhancements	121
Additional considerations	121
Restrictions	121
Incompatibilities	121
What this change affects	122
Migration procedures	122
SMTP exit to filter unwanted mail.	122
Restrictions	123
What this change affects	123
Migration procedures	123
Managed System Infrastructure (msys) for Setup	123
Restrictions	124

Dependencies	124
What this change affects	124
Migration procedures	124
Improve TCP/IP storage utilization management	124
Restrictions.	124
What this change affects	125
Migration procedures	125
Enterprise Extender performance enhancements	125
Restrictions.	125
What this change affects	125
Migration procedures	125
Enhanced CLAW packing	125
Restrictions.	126
What this change affects	126
Migration procedures	126
64-bit real addressing support	126
Restrictions.	127
Additional considerations	127
What this change affects	127
Migration procedures	127
OSA-Express token ring support	127
Restrictions.	128
What this change affects	128
Migration procedures	128
Changes to EZAZSSI	129
Restrictions.	129
What this change affects	129
Migration procedures	129
IPSec enhancements	130
Restrictions.	130
What this change affects	130
Migration procedures	130
TCP configuration options	130
Restrictions.	131
What this change affects	131
Migration procedures	131
Chapter 7. z/OS V1R1 Communications Server release summary	133
Chapter 8. Communications Server for OS/390 V2R10 release summary	135
Sysplex Distributor	135
Restrictions.	136
Incompatibilities	137
What this change affects	137
Migration procedures	137
Non-disruptive VIPA takeover	138
Restrictions.	138
What this change affects	138
Migration procedures	138
Policy-based network function enhancements	139
Policy Agent enhancements.	139
Service Level Policy Quality of Service (QoS) enhancements	141
Traffic Regulation and Management (TRM)	142
Queued Direct I/O (QDIO) queue management for MPCIPA devices	143
Restrictions.	144
What this change affects	144

Migration procedures	144
MPCIPA Queued Direct I/O enhancements for Fast Ethernet and ATM	
LAN-Emulation	144
Restrictions.	145
What this change affects	145
Migration procedures	145
MPCIPA Queued Direct I/O Address Resolution Protocol (ARP) cache	
enhancements.	146
Restrictions.	146
What this change affects	146
Migration procedures	146
syslogd isolation	146
Restrictions.	147
Incompatibilities	147
What this change affects	147
Migration procedures	147
Access control for ports, stack, and network.	148
Port access control	148
Stack access control	149
Network access control	150
Server bind control	151
Restrictions.	151
What this change affects	152
Migration procedures	152
On-demand tunnels.	152
Restrictions.	152
What this change affects	152
Migration procedures	152
REXEC enhancements	153
Restrictions.	153
What this change affects	153
Migration procedures	153
IPv6 API	153
Restrictions.	154
What this change affects	154
Migration procedures	154
High Speed Access Services (HSAS)	154
Restrictions.	154
What this change affects	154
Migration procedures	154
Express Logon feature: Digital Certificate Access Server (DCAS)	155
Restrictions.	155
What This Change Affects	155
Migration procedures	156
Serviceability enhancements	158
TCP/IP IPCS command enhancements	158
Socket API trace	159
TCP/IP trace enhancements	160
Performance improvements	160
Fast Local Sockets	160
Fast Response Cache Accelerator (FRCA) enhancement	161
IP Security (IPSec)	162
Route lookup improvements	162
CDLC device driver support for greater than 4K MTU	163
CLAW packing within a 4K frame.	164

	Chapter 9. Migrating the FTP server and client	167
	New and changed interfaces for FTP	167
	FTP server configuration statements	167
	FTP client configuration statements	170
	FTP z/OS UNIX and TSO commands	171
	FTP command start options.	174
	z/OS V1R4 Communications Server release summary	175
	FTP support for substitution characters during EBCDIC/ASCII single-byte	
	translations	175
	Enhanced FTP activity logging.	176
	Changed behavior of login failure replies	176
	Support for Chinese standard GB18030 provided by codepage IBM-5488	177
	Enhancements to FTP server user exits	178
	IPv6 support for FTP	180
	z/OS V1R2 Communications Server release summary	181
	Security enhancements	181
	Functional enhancements	186
	Communications Server for OS/390 V2R10 release summary	191
	FTP server	192
	FTP client	201
	Chapter 10. Migrating the Telnet server and client	203
	New and changed interfaces for Telnet	203
	Telnet PROFILE.TCPIP configuration file	203
	UNIX Telnet server (otelnetsd) configuration	209
	Telnet operator commands	209
	z/OS V1R4 Communications Server release summary	211
	Port qualification by linkname or destination IP address	211
	Printer enhancements	212
	Parameter placement enhancements	213
	New DEBUG option to suppress the connection dropped error messages	213
	New QINIT option for default applications.	214
	LU mapping enhancements	214
	Upgrade TN3270 SSL to use TLS	215
	z/OS V1R2 Communications Server release summary	216
	z/OS UNIX Telnet (otelnetsd) server – Kerberos support	216
	TN3270 diagnostics enhancements	217
	TN3270E RFC 2355 SNA extensions	218
	TN3270 profile and display enhancements	218
	Express Logon Feature using TN3270E Server on z/OS	221
	Communications Server for OS/390 V2R10 release summary	222
	The UNIX Telnet server (otelnetsd) enhancements.	222
	TN3270 SSL enhancement	223
	TN3270 System SSL	224
	TN3270 enhanced SLU simulation	225
	TN3270 NQN enhancement for the TN3270E server	226
	TN3270 client reconnect to TN3270E server	226
	TN3270E resource pooling	227
	TN3270 DEBUG	228
	TN3270 Timemark default change	228
	Chapter 11. Migrating the SNMP server and client	231
	SNMP overview	231
	Network management application	232
	SNMP agent	232
	SNMP subagents	232

	Key generation commands	233
	Distributed Protocol Interface	233
	Trap forwarder daemon	233
	New and changed interfaces for SNMP	234
	SNMP configuration files	234
	SNMP operator commands	234
	SNMP z/OS UNIX commands	235
	SNMP environment variables	235
	MIB modules	235
	z/OS V1R4 Communications Server release summary	236
	SNMP agent	236
	TCP/IP subagent.	236
	z/OS V1R2 Communications Server release summary	237
	SNMP agent	237
	TCP/IP subagent.	238
	Communications Server for OS/390 V2R10 release summary	240
	SNMP agent	240
	TCP/IP subagent.	243
	OMPRoute subagent	245
	Service Level Agreement subagent	245
	osnmp command	245
	NetView SNMP command	247
	SNMP Query Engine	247
	pwtokey command	247
	pwchange command	247
	Distributed Protocol Interface	247
	Trap forwarder daemon	248
	Chapter 12. Migrating to the BIND-based DNS name server	249
	New and changed interfaces for DNS	250
	DNS configuration files	250
	DNS z/OS UNIX commands	251
	DNS TSO commands	252
	DNS environment variables	252
	z/OS V1R4 Communications Server release summary	252
	Configuration file updates	253
	UNIX command updates	254
	Dependencies.	254
	Restrictions.	255
	What this change affects	255
	Migration procedures	255
	z/OS V1R2 Communications Server release summary	256
	BIND DNS upgrade.	256
	Communications Server for OS/390 V2R10 release summary	262
	DNS SRV Resource Record support	262
	DNS non-swappable mode support	263
	Appendix A. Migrating from Community-Based Security to SNMPv3	265
	Migrating the SNMP agent (osnmpd) configuration	265
	Migrating SNMP community entries from PW.SRC	265
	Migrating trap destination entries from SNMPTRAP.DEST	266
	Defining new users with the User-based Security Model	266
	Steps for migrating the osnmp command configuration	267
	Appendix B. Related protocol specifications (RFCs)	269
	Draft RFCs	276

Appendix C. Information APARs	279
Information APARs for IP documents	279
Information APARs for SNA documents	280
Other information APARs.	280
Appendix D. Accessibility	283
Using assistive technologies	283
Keyboard navigation of the user interface.	283
Notices	285
Trademarks.	288
Index	291
Communicating Your Comments to IBM	303

I

Figures

1. z/OS V1R4 Communications Server protocol suite	2
---	---

Tables

1. System management applications	9
2. Remote logon and file transfer applications	11
3. Remote printing applications.	11
4. Remote execution applications.	12
5. Routing applications.	12
6. Mail facility applications	13
7. Query resolution applications	13
8. Network computing applications	14
9. Miscellaneous application.	15
10. Programming tools and libraries	15
11. Distribution library data sets	16
12. Target library data sets	17
13. Shared distribution and target library data sets	18
14. Location of z/OS Communications Server HFS parts.	18
15. Migration roadmap	23
16. New or changed configuration files	29
17. New or changed TCPIP.DATA statements and parameters	31
18. New or changed PROFILE.TCPIP configuration statements and parameters	31
19. New or changed SYS1.PARMLIB members	35
20. New or changed operator commands	36
21. New or changed TSO commands.	43
22. New or changed UNIX commands	49
23. Environment variables	58
24. Socket APIs enabled for IPv6	58
25. Socket APIs.	59
26. CTRACE COMP(SYSTCPDA) subcommand.	61
27. INETSTAT subcommand	62
28. TCPIP.CS subcommand	63
29. Sysplex-wide Dynamic Source VIPAs for TCP connections - Migration task	67
30. Sysplexports - Migration task	68
31. Sysplex Wide Security Association (SWSA) - Migration task	69
32. Network access control - Migration tasks	70
33. FRCA access control - Migration tasks	70
34. Resolver enhancements - Migration tasks.	71
35. Event trace enhancements - Migration tasks.	73
36. TCP/IP support for Simple Network Time Protocol (SNTP) - Migration task	74
37. Ping enhancements - Migration tasks	76
38. Traceroute enhancements - Migration tasks	77
39. OSA Express: Amount of storage for read processing	78
40. HiperSockets: Amount of storage for read processing	78
41. New VTAM start options to adjust the QDIO or iQDIO storage - Migration tasks.	79
42. Enabling IPv6 support - Migration task	80
43. Configuration changes related to IPv6 support - Migration tasks	81
44. IPv6 support for resolver - Migration tasks	83
45. IPv6 support for Netstat - Migration task	85
46. IPv6 support for Ping - Migration tasks	85
47. IPv6 support for Traceroute - Migration tasks	86
48. IPv6 support for event trace enhancements - Migration tasks	87
49. IPv6 support for TCP/IP socket API commands - Migration task	88
50. Resolver enhancements - Migration tasks.	94
51. Intrusion Detection Services - Migration tasks	97
52. Sysplex Distributor policy enhancements - Migration tasks	98
53. Policy Agent enhancements - Migration tasks	100

54. OROUTED to OMPROUTE migration - Migration Task	103
55. OMPROUTE to allow RIP1 and RIP2 packets over the same interface - Migration tasks	104
56. Replaceable static routes - Migration tasks	105
57. Additional RIP filter for OMPROUTE- Migration task	106
58. OSPF MD5 authentication - Migration tasks	107
59. Native Socket API TCP_NODELAY support - Migration tasks	108
60. Restrict access to netstat command function - Migration task	110
61. Kerberos support for the UNIX RSHD server - Migration tasks.	111
62. Application-driven policy classification - Migration task.	112
63. VLAN priority tagging - Migration task.	113
64. HiperSockets - Migration tasks	115
65. Efficient routing using HiperSockets Accelerator - Migration tasks	118
66. Connection load balancing using Sysplex Distributor in a network with Cisco routers - Migration tasks	119
67. CICS sockets listener enhancements - Migration tasks	120
68. SMF recording enhancements - Migration tasks	122
69. SMTP exit to filter unwanted mail function - Migration tasks.	123
70. msys for Setup - Migration task	124
71. Improve TCP/IP storage utilization management function - Migration tasks	125
72. Enhanced CLAW packing function - Migration tasks	126
73. 64-bit real addressing support - Migration tasks	127
74. OSA-Express token ring support - Migration tasks	128
75. Changes to EZAZSSI - Migration task	129
76. IPsec performance enhancements - Migration task.	130
77. TCP configuration options enhancements - Migration tasks	131
78. Sysplex Distributor - Migration tasks	137
79. Non-disruptive VIPA takeover - Migration task to prevent enabling of the function.	139
80. Non-disruptive VIPA takeover - Optional migration tasks	139
81. Policy Agent and LDAP enhancements - Migration tasks.	141
82. Service Level Policy Quality of Service (QoS) enhancements - Migration tasks	142
83. Traffic Regulation and Management function - Migration tasks.	143
84. MPCIPA QDIO enhancements for Fast Ethernet and ATM LAN-Emulation - Migration tasks	145
85. MPCIPA QDIO ARP cache enhancements - Migration task	146
86. syslogd isolation - Migration tasks	147
87. Port access control - Migration tasks	149
88. Stack access control - Migration tasks	150
89. Network access control- Migration tasks	151
90. Server bind control - Migration tasks	152
91. REXEC - Migration tasks	153
92. IPv6 API - Migration tasks	154
93. High Speed Access Services - Migration tasks	154
94. Express Logon feature: DCAS - Migration tasks	156
95. TCP/IP IPCS command enhancements - Migration tasks.	159
96. Socket API trace - Migration tasks	160
97. TCP/IP trace enhancements - Migration tasks.	160
98. Fast Local Sockets - Migration tasks	161
99. Route lookup improvements - Migration tasks	163
100. CDLC device driver performance improvement - Migration tasks	164
101. CLAW packing within a 4K frame - Migration task	165
102. New and changed FTP server configuration statements	167
103. New and changed FTP client configuration statements	170
104. FTP z/OS UNIX and TSO commands.	171
105. FTP command start options	174
106. FTP support for substitution characters during EBCDIC/ASCII single-byte translations - Migration tasks.	176
107. Enhanced FTP activity logging - Migration tasks	176

	108. Changed behavior of login failure replies - Migration tasks if you want to override default behavior	177
	109. Support for Chinese standard GB18030 provided by codepage IBM-5488 - Migration tasks	178
	110. FTP parameters and user exits that are enhanced in z/OS CS V1R4	179
	111. Enhancements to FTP server user exits - Migration tasks	179
	112. IPv6 application for FTP - Migration tasks	181
	113. Enhancing FTP server security - Migration tasks	182
	114. Surrogate RACF support - Migration tasks	183
	115. Socksify FTP client - Migration Task	184
	116. TLS enablement for FTP - Migration tasks	184
	117. Kerberos support for the FTP server and client - Migration tasks	185
	118. ISPF statistics - Migration tasks	186
	119. User-level FTP server options - Migration task	187
	120. Stream mode restart - Migration tasks	188
	121. RFC 2389 Updates - Migration tasks	189
	122. RFC 2640 Updates - Migration tasks	190
	123. Native ASCII support - Migration tasks	191
	124. FTP trace enhancements - Migration tasks	191
	125. Welcome page support - Migration tasks	192
	126. Request e-mail address as a password for anonymous users - Migration task	194
	127. Extending SMF 118 record for byte transfer count - Migration Task	194
	128. Server anonymous enhancements using APAR PQ28980 - Migration tasks	195
	129. Server anonymous enhancements when <i>not</i> using APAR PQ28980 - Migration tasks	196
	130. Extensions to FTP: SIZE and MDTM function - Migration tasks	197
	131. Transfer MVS data sets with FTP URL - Migration tasks	198
	132. FTP SITE and LOCSITE allocation keywords - Migration tasks	199
	133. FTP JES - Migration tasks	200
	134. User exit enhancements - Migration tasks	201
	135. DDname support - Migration tasks	202
	136. PROFILE.TCPIP — TELNETGLOBAL configuration file (Telnet)	204
	137. PROFILE.TCPIP — TELNETPARMS configuration file (Telnet)	205
	138. PROFILE.TCPIP — BEGINVTAM configuration file (Telnet)	206
	139. New or changed Telnet configuration	209
	140. New or changed Telnet operator commands	209
	141. Port qualification by linkname or destination IP address - Migration tasks.	212
	142. Telnet printer enhancements - Migration tasks.	213
	143. DEBUG EXCEPTION option - Migration task	214
	144. Default application QINIT option - Migration task.	214
	145. LU mapping enhancements - Migration tasks	215
	146. Kerberos support for the UNIX Telnet server - Migration tasks	217
	147. TN3270 diagnostics enhancements - Migration tasks	218
	148. TN3270E RFC 2355 SNA extensions - Migration tasks	218
	149. TN3270 profile and display enhancements - Migration tasks	221
	150. Express Logon Feature using TN3270E server on z/OS function - Migration tasks	222
	151. otelnetd enhancements - Migration tasks	222
	152. TN3270 Negotiated SSL - Migration tasks	223
	153. TN3270 System SSL - Migration tasks	225
	154. TN3270 enhanced SLU simulation - Migration tasks	226
	155. TN3270 NQN enhancement for the TN3270E server - Migration tasks	226
	156. TN3270 client reconnect to TN3270E server - Migration task	227
	157. TN3270E resource pooling - Migration tasks	228
	158. TN3270 DEBUG function - Migration task	228
	159. TN3270 Timemark default change function - Migration task	229
	160. New or changed configuration files (SNMP)	234
	161. New or changed operator commands (SNMP)	234
	162. New or changed UNIX commands (SNMP).	235

163. New or changed environment variables (SNMP)	235
164. SNMP agent MIB modules	235
165. TCP/IP subagent MIB modules	236
166. Service Level Agreement subagent MIB modules	236
167. SNMP security enhancements - Migration task	237
168. SNMP Community MIB enhancement - Migration tasks	238
169. TCP/IP subagent in z/OS CS V1R2 - Migration tasks	240
170. UTF8 support - Migration task	241
171. Notification filtering support - Migration task	241
172. Inform support - Migration task	242
173. Encryption support - Migration task.	242
174. Environment variable support - Migration task.	243
175. Allow source VIPA - Migration tasks	243
176. TCP/IP Subagent in CS for OS/390 V2R10 - Migration tasks	245
177. Encryption support - Migration task.	246
178. osnmp environment variable support for CS for OS/390 V2R10 - Migration task	246
179. osnmp allow source VIPA for CS for OS/390 V2R10 - Migration tasks	246
180. SNMP Query Engine - Migration task	247
181. Trap forwarder daemon - Migration tasks	248
182. New or changed configuration files (DNS)	250
183. New or changed UNIX commands (DNS)	251
184. New or changed TSO commands (DNS).	252
185. Environment variables (DNS)	252
I 186. BIND 9.2 upgrades - Migration tasks	255
I 187. IPv6 DNS - Migration tasks for automatic rndc configuration for a local rndc client	256
188. Running the name server in BIND 9 mode only - Migration tasks.	259
189. Running the name server in 4.9.3 mode only - Migration task	261
190. Running the name server in BIND 9 mode and BIND 4.9.3 mode simultaneously - Migration tasks	261
191. DNS SRV RR support - Migration tasks	263
192. DNS non-swappable mode support - Migration tasks	263
193. IP information APARs.	279
194. SNA information APARs	280
195. Non-document information APARs	281

About this document

The purpose of this document is to describe the migration considerations for the TCP/IP component of z/OS™ Version 1 Release 4 Communications Server (z/OS CS), including the migration considerations from the following earlier releases of the TCP/IP product of IBM:

- z/OS V1R2 Communications Server
- Communications Server for OS/390® V2R10

Note: z/OS Communications Server did not ship new function in z/OS V1R1 or in z/OS V1R3.

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.

It is strongly recommended that you read *z/OS and z/OS.e Planning for Installation* in conjunction with this document.

z/OS Communications Server exploits z/OS UNIX® services even for traditional MVS™ environments and applications. Therefore, before using TCP/IP services, your installation must establish a full-function mode z/OS UNIX environment—including a Data Facility Storage Management Subsystem (DFSMSdfp™), a Hierarchical File System (HFS), and a security product (such as Resource Access Control Facility, or RACF®)—before z/OS Communications Server can be started successfully. Refer to *z/OS UNIX System Services Planning* for more information.

Throughout this document when the term RACF is used, it means RACF or an SAF-compliant security product.

For an overview of the VTAM® component of z/OS Communications Server, refer to *z/OS Communications Server: SNA Network Implementation Guide*.

For comments and suggestions about this document, use the Reader's Comment Form located at the back of this document. This form provides instructions on submitting your comments by mail, by fax, or by electronic mail.

This document supports z/OS.e™.

Who should use this document

This document is designed for planners, system programmers, and network administrators who are planning to install z/OS Communications Server and who want to learn more about its new and enhanced features.

You need to be familiar with Transmission Control Protocol/Internet Protocol (TCP/IP) and the Multiple Virtual Storage (MVS) platform to use this document.

How this document is organized

All users should read the following:

- Chapter 1, “Overview of z/OS Communications Server” on page 1 provides an overview of the z/OS Communications Server protocol suite along with a discussion of installation.
- Chapter 2, “Migration overview” on page 23 provides a roadmap that includes each release’s functional enhancements, whether enabling or migration actions are required, and page references. This chapter also provides a migration checklist, which you can tailor to meet the specific requirements of your installation.
- Chapter 3, “New and changed interfaces” on page 29 provides tables that include new, changed, deleted, or obsolete statements, commands, and APIs, and other interfaces.

You should also read each release summary chapter for every release in your migration path so that you are aware of all the enhancements and changes introduced since your last installation.

The following chapters summarize the IP functions and migration procedures:

- Chapter 4, “z/OS V1R4 Communications Server release summary” on page 65
- Chapter 5, “z/OS V1R3 Communications Server release summary” on page 89
- Chapter 6, “z/OS V1R2 Communications Server release summary” on page 91
- Chapter 7, “z/OS V1R1 Communications Server release summary” on page 133
- Chapter 8, “Communications Server for OS/390 V2R10 release summary” on page 135

The preceding chapters describe migration considerations for all applications except File Transfer Protocol (FTP), Telnet, Simple Network Management Protocol (SNMP), and Domain Name System (DNS) name server. Migration considerations for these applications are covered in the following chapters:

- Chapter 9, “Migrating the FTP server and client” on page 167
- Chapter 10, “Migrating the Telnet server and client” on page 203
- Chapter 11, “Migrating the SNMP server and client” on page 231
- Chapter 12, “Migrating to the BIND-based DNS name server” on page 249

Appendix A, “Migrating from Community-Based Security to SNMPv3” on page 265 describes the steps to take when migrating from community-based security to SNMPv3.

Where to find more information

This section contains:

- Pointers to information available on the Internet
- Information about licensed documentation
- Information about LookAt, the online message tool
- A set of tables that describes the documents in the z/OS Communications Server (z/OS CS) library, along with related publications

Where to find related information on the Internet

z/OS

- <http://www.ibm.com/servers/eserver/zseries/zos/>

z/OS Internet Library

- <http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>

IBM Communications Server product

- <http://www.software.ibm.com/network/commsserver/>

IBM Communications Server product support

- <http://www.software.ibm.com/network/commsserver/support/>

IBM Systems Center publications

- <http://www.redbooks.ibm.com/>

IBM Systems Center flashes

- <http://www-1.ibm.com/support/techdocs/atmsmastr.nsf>

RFCs

- <http://www.ietf.org/rfc.html>

RFC drafts

- <http://www.ietf.org/ID.html>

Information about Web addresses can also be found in information APAR I11334.

DNS web sites

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

USENET news groups:

`comp.protocols.dns.bind`

For BIND mailing lists, see:

- <http://www.isc.org/ml-archives/>
 - 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 (Note: This list may 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.

For definitions of the terms and abbreviations used in this document, you can view or download the latest *IBM Glossary of Computing Terms* at the following Web address:

<http://www.ibm.com/ibm/terminology>

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

Accessing z/OS licensed documents on the Internet

z/OS licensed documentation is available on the Internet in PDF format at the IBM Resource Link™ Web site at:

<http://www.ibm.com/servers/resourceLink>

Licensed documents are available only to customers with a z/OS license. Access to these documents requires an IBM Resource Link user ID and password, and a key code. With your z/OS order you received a Memo to Licensees, (GI10-0671), that includes this key code.

To obtain your IBM Resource Link user ID and password, log on to:

<http://www.ibm.com/servers/resourceLink>

To register for access to the z/OS licensed documents:

1. Sign in to Resource Link using your Resource Link user ID and password.
2. Select **User Profiles** located on the left-hand navigation bar.

Note: You cannot access the z/OS licensed documents unless you have registered for access to them and received an e-mail confirmation informing you that your request has been processed.

Printed licensed documents are not available from IBM.

You can use the PDF format on either **z/OS Licensed Product Library CD-ROM** or IBM Resource Link to print licensed documents.

Using LookAt to look up message explanations

LookAt is an online facility that allows you to look up explanations for most messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can access LookAt from the Internet at:

<http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/>

or from anywhere in z/OS where you can access a TSO/E command line (for example, TSO/E prompt, ISPF, z/OS UNIX System Services running OMVS). You can also download code from the *z/OS Collection* (SK3T-4269) and the LookAt Web site that will allow you to access LookAt from a handheld computer (Palm Pilot VIIx suggested).

To use LookAt as a TSO/E command, you must have LookAt installed on your host system. You can obtain the LookAt code for TSO/E from a disk on your *z/OS Collection* (SK3T-4269) or from the **News** section on the LookAt Web site.

Some messages have information in more than one document. For those messages, LookAt displays a list of documents in which the message appears.

How to contact IBM service

For immediate assistance, visit this Web site:
<http://www.software.ibm.com/network/commserver/support/>

Most problems can be resolved at this Web site, where you can submit questions and problem reports electronically, as well as 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 (1-800-237-5511). You will receive a return call within 8 business hours (Monday – Friday, 8:00 a.m. – 5:00 p.m., local customer time).

Outside of 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 303.

z/OS Communications Server information

This section contains descriptions of the documents in the z/OS Communications Server library.

z/OS Communications Server publications are available:

- Online at the z/OS Internet Library web page at <http://www.ibm.com/servers/eserver/zseries/zos/bkserv>
- In softcopy on CD-ROM collections.

Softcopy information

Softcopy publications are available in the following collections:

Titles	Order Number	Description
<i>z/OS V1R4 Collection</i>	SK3T-4269	This is the CD collection shipped with the z/OS product. It includes the libraries for z/OS V1R4, in both BookManager® and PDF formats.
<i>z/OS Software Products Collection</i>	SK3T-4270	This CD includes, in both BookManager and PDF formats, the libraries of z/OS software products that run on z/OS but are not elements and features, as well as the <i>Getting Started with Parallel Sysplex</i> ® bookshelf.
<i>z/OS V1R4 and Software Products DVD Collection</i>	SK3T-4271	This collection includes the libraries of z/OS (the element and feature libraries) and the libraries for z/OS software products in both BookManager and PDF format. This collection combines SK3T-4269 and SK3T-4270.
<i>z/OS Licensed Product Library</i>	SK3T-4307	This CD includes the licensed documents in both BookManager and PDF format.
<i>System Center Publication IBM S/390® Redbooks™ Collection</i>	SK2T-2177	This collection contains over 300 ITSO redbooks that apply to the S/390 platform and to host networking arranged into subject bookshelves.

z/OS Communications Server library

z/OS V1R4 Communications Server documents are available on the CD-ROM accompanying z/OS (SK3T-4269 or SK3T-4307). Unlicensed documents can be viewed at the z/OS Internet library site.

Updates to documents are available on RETAIN® and in information APARs (info APARs). See Appendix C, “Information APARs” on page 279 for a list of the documents and the info APARs associated with them.

- Info APARs for OS/390 documents are in the document called *OS/390 DOC APAR and PTF ++HOLD Documentation* which can be found at http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/IDDOCMST/CCONTENTS.
- Info APARs for z/OS documents are in the document called *z/OS and z/OS.e DOC APAR and PTF ++HOLD Documentation* which can be found at http://publibz.boulder.ibm.com:80/cgi-bin/bookmgr_OS390/BOOKS/ZIDOCMST/CCONTENTS.

Planning and migration:

Title	Number	Description
<i>z/OS Communications Server: SNA Migration</i>	GC31-8774	This document is intended to help you plan for SNA, whether you are migrating from a previous version or installing SNA for the first time. This document also identifies the optional and required modifications needed to enable you to use the enhanced functions provided with SNA.
<i>z/OS Communications Server: IP Migration</i>	GC31-8773	This document is intended to help you plan for TCP/IP Services, whether you are migrating from a previous version or installing IP for the first time. This document also identifies the optional and required modifications needed to enable you to use the enhanced functions provided with TCP/IP Services.
<i>z/OS Communications Server: IPv6 Network and Application Design Guide</i>	SC31-8885	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
<i>z/OS Communications Server: IP Configuration Guide</i>	SC31-8775	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 in conjunction with the <i>z/OS Communications Server: IP Configuration Reference</i> .
<i>z/OS Communications Server: IP Configuration Reference</i>	SC31-8776	This document presents information for people who want to administer and maintain IP. Use this document in conjunction with the <i>z/OS Communications Server: IP Configuration Guide</i> . The information in this document includes: <ul style="list-style-type: none"> • TCP/IP configuration data sets • Configuration statements • Translation tables • SMF records • Protocol number and port assignments
<i>z/OS Communications Server: SNA Network Implementation Guide</i>	SC31-8777	This document presents the major concepts involved in implementing an SNA network. Use this document in conjunction with the <i>z/OS Communications Server: SNA Resource Definition Reference</i> .
<i>z/OS Communications Server: SNA Resource Definition Reference</i>	SC31-8778	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 in conjunction with the <i>z/OS Communications Server: SNA Network Implementation Guide</i> .
<i>z/OS Communications Server: SNA Resource Definition Samples</i>	SC31-8836	This document contains sample definitions to help you implement SNA functions in your networks, and includes sample major node definitions.
<i>z/OS Communications Server: AnyNet SNA over TCP/IP</i>	SC31-8832	This guide provides information to help you install, configure, use, and diagnose SNA over TCP/IP.
<i>z/OS Communications Server: AnyNet Sockets over SNA</i>	SC31-8831	This guide provides information to help you install, configure, use, and diagnose sockets over SNA. It also provides information to help you prepare application programs to use sockets over SNA.

Title	Number	Description
<i>z/OS Communications Server: IP Network Print Facility</i>	SC31-8833	This document is for system 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
<i>z/OS Communications Server: IP User's Guide and Commands</i>	SC31-8780	This document describes how to use TCP/IP applications. It contains requests that allow a user to log on to a remote host using Telnet, transfer data sets using FTP, send and receive electronic mail, print on remote printers, and authenticate network users.
<i>z/OS Communications Server: IP System Administrator's Commands</i>	SC31-8781	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.
<i>z/OS Communications Server: SNA Operation</i>	SC31-8779	This document serves as a reference for programmers and operators requiring detailed information about specific operator commands.
<i>z/OS Communications Server: Quick Reference</i>	SX75-0124	This document contains essential information about SNA and IP commands.

Customization:

Title	Number	Description
<i>z/OS Communications Server: SNA Customization</i>	LY43-0092	This document enables you to customize SNA, and includes the following: <ul style="list-style-type: none"> • 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
<i>z/OS Communications Server: IP Application Programming Interface Guide</i>	SC31-8788	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.
<i>z/OS Communications Server: IP CICS Sockets Guide</i>	SC31-8807	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.

Title	Number	Description
<i>z/OS Communications Server: IP IMS Sockets Guide</i>	SC31-8830	This document is for programmers who want application programs that use the IMS™ TCP/IP application development services provided by IBM's TCP/IP Services.
<i>z/OS Communications Server: IP Programmer's Reference</i>	SC31-8787	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.
<i>z/OS Communications Server: SNA Programming</i>	SC31-8829	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.
<i>z/OS Communications Server: SNA Programmer's LU 6.2 Guide</i>	SC31-8811	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.)
<i>z/OS Communications Server: SNA Programmer's LU 6.2 Reference</i>	SC31-8810	This document provides reference material for the SNA LU 6.2 programming interface for host application programs.
<i>z/OS Communications Server: CSM Guide</i>	SC31-8808	This document describes how applications use the communications storage manager.
<i>z/OS Communications Server: CMIP Services and Topology Agent Guide</i>	SC31-8828	This document describes the Common Management Information Protocol (CMIP) programming interface for application programmers to use in coding CMIP application programs. The document provides guide and reference information about CMIP services and the SNA topology agent.

Diagnosis:

Title	Number	Description
<i>z/OS Communications Server: IP Diagnosis</i>	GC31-8782	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.
<i>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</i>	LY43-0088 LY43-0089	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.
<i>z/OS Communications Server: SNA Data Areas Volume 1 and z/OS Communications Server: SNA Data Areas Volume 2</i>	LY43-0090 LY43-0091	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
<i>z/OS Communications Server: SNA Messages</i>	SC31-8790	This document describes the ELM, IKT, IST, ISU, IUT, IVT, and USS messages. Other information in this document includes: <ul style="list-style-type: none"> • Command and RU types in SNA messages • Node and ID types in SNA messages • Supplemental message-related information
<i>z/OS Communications Server: IP Messages Volume 1 (EZA)</i>	SC31-8783	This volume contains TCP/IP messages beginning with EZA.
<i>z/OS Communications Server: IP Messages Volume 2 (EZB)</i>	SC31-8784	This volume contains TCP/IP messages beginning with EZB.
<i>z/OS Communications Server: IP Messages Volume 3 (EZY)</i>	SC31-8785	This volume contains TCP/IP messages beginning with EZY.
<i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>	SC31-8786	This volume contains TCP/IP messages beginning with EZZ and SNM.
<i>z/OS Communications Server: IP and SNA Codes</i>	SC31-8791	This document describes codes and other information that appear in z/OS Communications Server messages.

APPC Application Suite:

Title	Number	Description
<i>z/OS Communications Server: APPC Application Suite User's Guide</i>	SC31-8809	This documents the end-user interface (concepts, commands, and messages) for the AFTP, ANAME, and APING facilities of the APPC application suite. Although its primary audience is the end user, administrators and application programmers may also find it useful.
<i>z/OS Communications Server: APPC Application Suite Administration</i>	SC31-8835	This document contains the information that administrators need to configure the APPC application suite and to manage the APING, ANAME, AFTP, and A3270 servers.
<i>z/OS Communications Server: APPC Application Suite Programming</i>	SC31-8834	This document provides the information application programmers need to add the functions of the AFTP and ANAME APIs to their application programs.

Redbooks

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

Title	Number
<i>TCP/IP Tutorial and Technical Overview</i>	GG24-3376
<i>SNA and TCP/IP Integration</i>	SG24-5291
<i>IBM Communications Server for OS/390 V2R10 TCP/IP Implementation Guide: Volume 1: Configuration and Routing</i>	SG24-5227
<i>IBM Communications Server for OS/390 V2R10 TCP/IP Implementation Guide: Volume 2: UNIX Applications</i>	SG24-5228
<i>IBM Communications Server for OS/390 V2R7 TCP/IP Implementation Guide: Volume 3: MVS Applications</i>	SG24-5229
<i>Secureway Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements</i>	SG24-5631
<i>TCP/IP in a Sysplex</i>	SG24-5235
<i>Managing OS/390 TCP/IP with SNMP</i>	SG24-5866

Title	Number
<i>Security in OS/390-based TCP/IP Networks</i>	SG24-5383
<i>IP Network Design Guide</i>	SG24-2580
<i>Migrating Subarea Networks to an IP Infrastructure</i>	SG24-5957
<i>IBM Communication Controller Migration Guide</i>	SG24-6298

Related information

For information about z/OS products, refer to *z/OS Information Roadmap* (SA22-7500). The Roadmap describes what level of documents are supplied with each release of z/OS Communications Server, as well as describing each z/OS publication.

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 table below lists documents that may be helpful to readers.

Title	Number
<i>z/OS Security Server Firewall Technologies</i>	SC24-5922
<i>S/390: OSA-Express Customer's Guide and Reference</i>	SA22-7403
<i>z/OS JES2 Initialization and Tuning Guide</i>	SA22-7532
<i>z/OS MVS Diagnosis: Procedures</i>	GA22-7587
<i>z/OS MVS Diagnosis: Reference</i>	GA22-7588
<i>z/OS MVS Diagnosis: Tools and Service Aids</i>	GA22-7589
<i>z/OS Security Server LDAP Client Programming</i>	SC24-5924
<i>z/OS Security Server LDAP Server Administration and Use</i>	SC24-5923
<i>Understanding LDAP</i>	SG24-4986
<i>z/OS UNIX System Services Programming: Assembler Callable Services Reference</i>	SA22-7803
<i>z/OS UNIX System Services Command Reference</i>	SA22-7802
<i>z/OS UNIX System Services User's Guide</i>	SA22-7801
<i>z/OS UNIX System Services Planning</i>	GA22-7800
<i>z/OS MVS Using the Subsystem Interface</i>	SA22-7642
<i>z/OS C/C++ Run-Time Library Reference</i>	SA22-7821
<i>z/OS Program Directory</i>	GI10-0670
<i>DNS and BIND</i> , Fourth Edition, O'Reilly and Associates, 2001	ISBN 0-596-00158-4
<i>Routing in the Internet</i> , Christian Huitema (Prentice Hall PTR, 1995)	ISBN 0-13-132192-7
<i>sendmail</i> , Bryan Costales and Eric Allman, O'Reilly and Associates, 1997	ISBN 156592-222-0
<i>TCP/IP Tutorial and Technical Overview</i>	GG24-3376
<i>TCP/IP Illustrated, Volume I: The Protocols</i> , W. Richard Stevens, Addison-Wesley Publishing, 1994	ISBN 0-201-63346-9
<i>TCP/IP Illustrated, Volume II: The Implementation</i> , Gary R. Wright and W. Richard Stevens, Addison-Wesley Publishing, 1995	ISBN 0-201-63354-X
<i>TCP/IP Illustrated, Volume III</i> , W. Richard Stevens, Addison-Wesley Publishing, 1995	ISBN 0-201-63495-3
<i>z/OS System Secure Sockets Layer Programming</i>	SC24-5901

Determining if a publication is current

As needed, IBM updates its publications with new and changed information. For a given publication, updates to the hardcopy and associated BookManager softcopy are usually available at the same time. Sometimes, however, the updates to hardcopy and softcopy are available at different times. The following information describes how to determine if you are looking at the most current copy of a publication:

- At the end of a publication's order number there is a dash followed by two digits, often referred to as the dash level. A publication with a higher dash level is more current than one with a lower dash level. For example, in the publication order number GC28-1747-07, the dash level 07 means that the publication is more current than previous levels, such as 05 or 04.
- If a hardcopy publication and a softcopy publication have the same dash level, it is possible that the softcopy publication is more current than the hardcopy publication. Check the dates shown in the Summary of Changes. The softcopy publication might have a more recently dated Summary of Changes than the hardcopy publication.
- To compare softcopy publications, you can check the last two characters of the publication's filename (also called the book name). The higher the number, the more recent the publication. Also, next to the publication titles in the CD-ROM booklet and the readme files, there is an asterisk (*) that indicates whether a publication is new or changed.

Summary of changes

Summary of changes for GC31-8773-02 z/OS Version 1 Release 4

This document contains information previously presented in GC31-8773-01, which supports z/OS Version 1 Release 2. 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.

New information

- Chapter 4, “z/OS V1R4 Communications Server release summary” on page 65 includes descriptions and migration procedures for all new functions and enhancements introduced in this release.

The new functions and enhancements pertain to IPv4 addressing unless specifically identified to be IPv6. This release introduces support for IPv6 addressing for certain functions and applications; see “IPv6 support” on page 79 for migration information that is pertinent if you choose to use the IPv6 support.

An appendix with z/OS product accessibility information has been added.

Changed information

- Chapter 1, “Overview of z/OS Communications Server” on page 1 is updated to reflect changes introduced in this release.
- Chapter 2, “Migration overview” on page 23 is expanded to include z/OS V1R4 Communications Server functional enhancements. In addition, the name of the chapter is changed from “Migration Roadmap” to “Migration overview” because the chapter provides the planning and migration checklist as well as the roadmap.
- Chapter 3, “New and changed interfaces” on page 29 is expanded to include the external interfaces that are new or changed as a result of z/OS V1R4 Communications Server functions.
- Chapter 9, “Migrating the FTP server and client” on page 167 is expanded to include a section for z/OS V1R4 Communications Server FTP functions and migration procedures. The new and changed FTP external interfaces are also included in this chapter.
- Chapter 10, “Migrating the Telnet server and client” on page 203 is expanded to include a section for z/OS V1R4 Communications Server Telnet functions and migration procedures. The new and changed Telnet external interfaces are also included in this chapter.
- Chapter 11, “Migrating the SNMP server and client” on page 231 is expanded to include a section for z/OS V1R4 Communications Server SNMP functions and migration procedures. The new and changed SNMP external interfaces are also included in this chapter.
- Chapter 12, “Migrating to the BIND-based DNS name server” on page 249 is expanded to include a section for z/OS V1R4 Communications Server DNS functions and migration procedures. The new and changed DNS external interfaces are also included in this chapter.

Moved information

- The information that was previously in Appendix B, "Planning Your Migration" is now contained elsewhere in the document. Specifically, the content of the Reference Books table is now merged into "z/OS Communications Server information" on page xxiii and the planning and migration checklist is now part of Chapter 2, "Migration overview" on page 23.

Deleted information

- The chapters and sections documenting functions and enhancements for OS/390 V2R8, Communications Server for OS/390 V2R7, and Communications Server for OS/390 V2R6 were removed from this document because migrating from those releases is not supported in z/OS CS V1R4 and beyond. You can still access the old information by referring to *z/OS IBM Communications Server: IP Migration Version 1 Release 2* at the following Web site:
<http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>.

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

Starting with z/OS V1R4, you may notice that headings use uppercase for the first letter of initial words only. This style change reflects an ongoing improvement to the consistency of our documents.

This document supports z/OS.e.

Summary of changes for GC31-8773-01 z/OS Version 1 Release 2

This document contains information previously presented in GC31-8773-00, which supports z/OS Version 1 Release 1.

New information

- Chapter 6, "z/OS V1R2 Communications Server release summary" on page 91. It includes descriptions and migration procedures of all new functions and enhancements introduced in this release.

Changed information

- Chapter 1, "Overview of z/OS Communications Server" on page 1 is updated to reflect changes introduced in this release.
- Chapter 2, "Migration overview" on page 23 is expanded to include z/OS V1R2 Communications Server functional enhancements.
- Chapter 3, "New and changed interfaces" on page 29 is expanded to include the external interfaces that are new or changed as a result of z/OS V1R2 Communications Server functions.
- Chapter 9, "Migrating the FTP server and client" on page 167 is expanded to include a section for z/OS V1R2 Communications Server FTP functions and migration procedures. The new and changed FTP external interfaces are also included in this chapter.
- Chapter 10, "Migrating the Telnet server and client" on page 203 is expanded to include a section for z/OS V1R2 Communications Server Telnet functions and migration procedures. The new and changed Telnet external interfaces are also included in this chapter.

- Chapter 11, “Migrating the SNMP server and client” on page 231 is expanded to include a section for z/OS V1R2 Communications Server SNMP functions and migration procedures. The new and changed SNMP external interfaces are also included in this chapter.
- Chapter 12, “Migrating to the BIND-based DNS name server” on page 249 is expanded to include a section for z/OS V1R2 Communications Server DNS functions and migration procedures. The new and changed DNS external interfaces are also included in this chapter.

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

**Summary of changes
for GC31-8773-00
z/OS Version 1 Release 1**

This document contains information also presented in *OS/390 V2R10 IBM Communications Server: IP Migration*.

New information

- Chapter 7, “z/OS V1R1 Communications Server release summary” on page 133.

Changed information

This document differs from its predecessor, *OS/390 V2R10 IBM Communications Server: IP Migration* in the following ways:

- The chapters and sections documenting functions and enhancements introduced prior to CS for OS/390 V2R6 are removed from this document because migrating from CS for OS/390 V2R5 and before is not supported in z/OS CS V1R1 and beyond. You can still access the old information; refer to “Where to find related information on the Internet” on page xx for Web addresses.
- The discussions on the OS/390 UNIX environment, OS/390 UNIX security considerations, and common OS/390 UNIX configuration problems that were previously in the CS for OS/390 V2R5 Release Summary chapter were moved into the configuration manuals. Furthermore, OS/390 UNIX is now called z/OS UNIX. Refer to *z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide* for information on these topics.

Chapter 1. Overview of z/OS Communications Server

z/OS Communications Server provides a set of communications protocols that support peer-to-peer connectivity functions for both local and wide-area networks, including the most popular wide-area network, the Internet. z/OS Communications Server also provides performance enhancements that can benefit a variety of TCP/IP applications.

Note: For the purposes of this library, zSeries is defined to mean the hardware that is known as the IBM S/390 Parallel Enterprise Server Generation 5 (G5) and Generation 6 (G6), the IBM S/390 Multiprise 3000 Enterprise Server, as well as the IBM @server zSeries 800 (z800) and 900 (z900).

This chapter covers the following topics:

- “What is z/OS Communications Server?”
- “TCP/IP packaging process” on page 16
- “Encryption features” on page 20

What is z/OS Communications Server?

z/OS Communications Server provides both SNA and TCP/IP networking protocols for z/OS. The SNA protocols are provided by VTAM and include Subarea, Advanced Peer-to-Peer Networking®, and High Performance Routing protocols. For more information on z/OS Communications Server SNA protocols, refer to *z/OS Communications Server: SNA Network Implementation Guide*.

Figure 1 on page 2 shows the z/OS V1R4 Communications Server TCP/IP protocol suite (also called *stack*), whose functions include associated applications, transport- and network-protocol layers, and connectivity and gateway functions. z/OS V1R4 Communications Server contains IPv6 support. Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for more detailed information.

The z/OS V1R4 Communications Server protocol suite supports two environments:

- A native MVS environment in which users can exploit the popular TCP/IP protocols in MVS application environments such as batch jobs, started tasks, TSO, CICS applications, and IMS applications.
- A z/OS UNIX System Services (z/OS UNIX) environment that lets you create and use applications that conform to the POSIX or XPG4 standard (a UNIX specification). See *z/OS Communications Server: IP Configuration Guide* for UNIX considerations.

Note: z/OS Communications Server exploits z/OS UNIX services even for traditional MVS environments and applications. Prior to utilizing TCP/IP services, therefore, a full-function mode z/OS UNIX environment—including a Data Facility Storage Management Subsystem (DFSMSdftp), a Hierarchical File System (HFS), and a security product (such as Resource Access Control Facility, or RACF)—needs to be defined and active before z/OS Communications Server can be started successfully.

z/OS CS

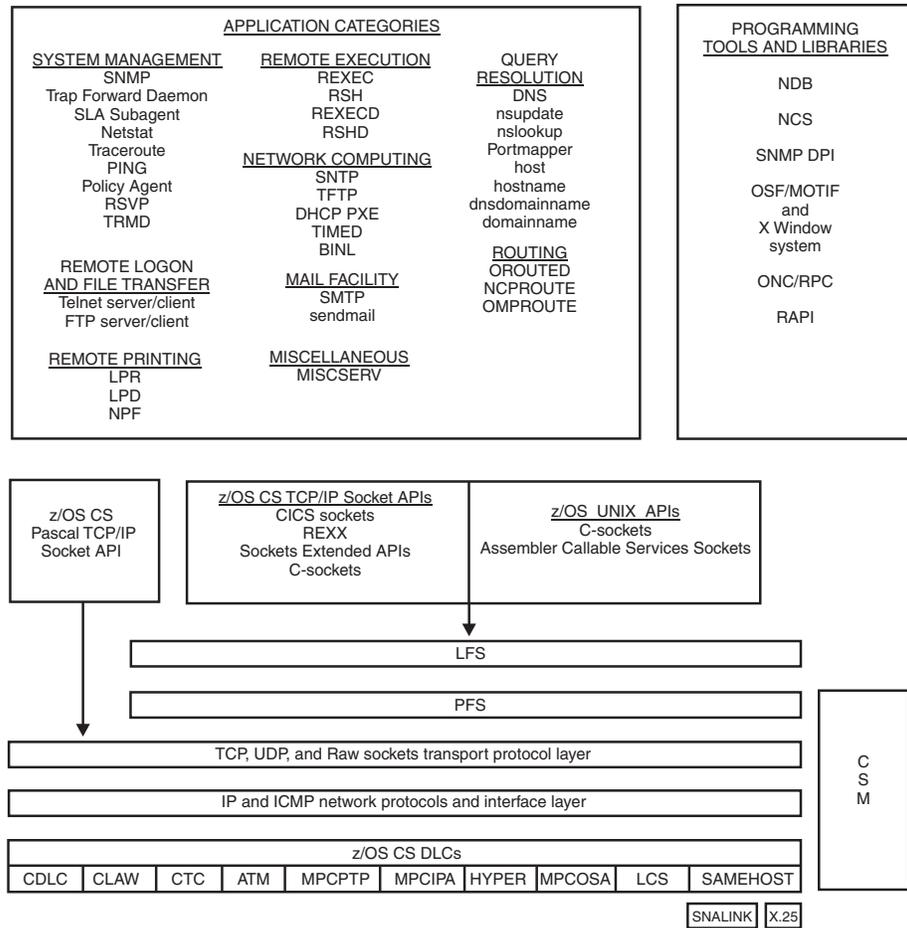


Figure 1. z/OS V1R4 Communications Server protocol suite

z/OS V1R4 Communications Server protocol-suite functions can be grouped in the following eight categories:

- “TCP/IP protocol stack”
- “Connectivity and gateway functions” on page 3
- “Network protocol layer” on page 4
- “Transport layer” on page 5
- “File systems” on page 5
- “Application Programming Interfaces (APIs)” on page 6
- “Applications” on page 8
- “Programming tools and libraries” on page 15

The following sections describe each of these functional categories.

TCP/IP protocol stack

The Transmission Control Protocol (TCP) and the Internet Protocol (IP) refer to a non-proprietary protocol suite that enables different packet-switched networks to function as a single entity regardless of underlying network topology.

z/OS V1R4 Communications Server provides robustness and high performance with the following features:

- A fully multiprocessor capable stack
- Exploitation of MVS Reliability, Availability, and Serviceability (RAS) services
- Exploitation of the z/OS architecture to optimize performance, CPU utilization, and throughput
- Exploitation of the z/OS Sysplex functions to maximize availability and scalability of TCP/IP workloads

In addition, z/OS V1R4 Communications Server design includes a tightly integrated storage and I/O model. I/O is provided by multipath channel (MPC) for network communication; storage management is provided by Communications Storage Manager (CSM). MPC and CSM are discussed in the following sections.

Multipath channel (MPC) I/O process

The term multipath channel (MPC) describes all z/OS Communications Server I/O driver support. There are specific I/O drivers under this support that are also referred to as MPC (such as MPCPTP).

MPC is a component of the I/O process model. MPC handles protocol headers and data separately and executes multiple I/O dispatchable units of work. MPC provides support for all devices supported by z/OS V1R4 Communications Server. The MPC I/O process and the CSM facilities that TCP/IP exploits are part of the VTAM component of z/OS V1R4 Communications Server. **As a result, VTAM must be configured and active when starting devices on the TCP/IP stack.**

Communications Storage Management (CSM)

The CSM facility is used by authorized programs to manage subsystem storage pools. CSM reduces data moves by providing a flat storage model that is accessible at multiple layers of the process model and across MVS address space boundaries. In addition, CSM provides the following technical advantages:

- MVS cellpool-like services
- Automatic handling of the contraction and expansion of storage resources
- Handling of different types and sizes of storage requests (for example, pageable and fixed)

Connectivity and gateway functions

TCP/IP connectivity and gateway functions handle the physical interfaces and the routing of IP data packets called *datagrams*. The following communication interfaces are supported by z/OS V1R4 Communications Server:

- ATM** Enables TCP/IP to send data to an asynchronous transfer mode (ATM) network using an OSA-2 or OSA-Express ATM adapter over an ATM virtual circuit.
- CDLC** Provides connectivity to a Network Control Program (NCP) through 3745/3746 network Front End Processor (FEP) controllers.
- CLAW** Provides access from IBM RS/6000® workstations directly to TCP/IP hosts over a channel. The CLAW (common link access to workstation) interface can also be used to provide connectivity to the original equipment manufacturer (OEM), such as the Cisco Channel Interface Processor (CIP).
- CTC** Provides access to TCP/IP hosts by way of a channel-to-channel (CTC) connection established over a zSeries™ ESCON® channel.

HYPERchannel

Provides access to TCP/IP hosts by way of HYPERchannel series A devices and series DX devices that function as series A devices.

LCS Provides access to TCP/IP hosts using the following devices:

- An IBM 3172 Interconnect Controller, which connects to a token ring, an Ethernet, or FDDI local area network
- An IBM 8232
- An IBM 2216 Multiaccess Connector Model 400
- An FDDI, Ethernet, Fast Ethernet, or Token Ring OSA or OSA-2 adapter
- An ATM OSA-2 in LAN emulation mode

MPCIPA

Provides access to TCP/IP hosts using the following:

- OSA-Express adapter with the Queued Direct I/O (QDIO) interface. OSA-Express supports the QDIO architecture for Gigabit Ethernet, Fast Ethernet, ATM LAN-Emulation attachment, and Token Ring. OSA-Express also supports IPv6 for Gigabit Ethernet and Fast Ethernet.
- HiperSockets using the Internal Queued Direct I/O (iQDIO). HiperSockets provides high-speed, low-latency IP message passing between Logical Partitions (LPARs) within a single IBM @server z/Series z800 or z900 server.

MPCOSA

Provides access to TCP/IP hosts by way of OSA-2 configured in HPDT MPC mode for Fast Ethernet or FDDI.

MPCPTP

Provides access to TCP/IP hosts through Multi-Path Channel Point-To-Point (MPCPTP) links. MPCPTP can be used in two ways to provide direct connectivity to other mainframe hosts running OS/390 or z/OS Communications Server:

- By using a set of two or more zSeries channels
- By configuring to utilize XCF services, if the zSeries hosts are part of the same sysplex

MPCPTP can also be used to provide the following connectivity options:

- Direct communication between two z/OS Communications Server TCP/IP Services protocol stacks running on the same MVS host without requiring any network attachments
- Connectivity to network attachments such as the IBM 2216 Multiaccess Controller Model 400 or the IBM RS/6000

SAMEHOST

Provides connectivity between the TCP/IP address space and other program address spaces within the same MVS host. The SAMEHOST Data Link Control (DLC) provides support for the SNA backbone network (SNALINK LU0 and SNALINK LU6.2) and the X.25 network.

Network protocol layer

The network protocol layer provides the support for the IP protocol. All TCP and User Datagram Protocol (UDP) data goes through the IP layer when entering and leaving the host. TCP and UDP will use the IPv4 routing layer or the IPv6 routing layer.

The network layer also provides support for the Internet Control Message Protocol (ICMP) and ICMPv6. This is used by the IP layer to exchange information and error messages with IP layers on other hosts and routers. ICMP is used for the IPv4 protocol and ICMPv6 is used for the IPv6 protocol.

Transport layer

The transport layer provides the support for the TCP, UDP, and RAW protocols. All three protocols use IPv4 or IPv6 as the network layer. The TCP protocol provides a connection-oriented, reliable transport layer, whereas UDP provides a simpler, connectionless and unreliable transport layer. The RAW transport layer provides for a more direct interface to the IP layer, which is primarily used by system-management type applications.

File systems

The file system layer provides the main interface between the Application Programming Interfaces (APIs) and the transport layers. The first component of the file system layer is the z/OS UNIX Logical File System (LFS). The LFS provides the API layer with a common interface to access files and sockets. In a POSIX-compliant environment, applications can access both files and sockets in a similar fashion. For example, both files and sockets are represented by a 16-bit integer referred to as a descriptor. Common functions can be used to access both file and socket resources.

The layer beneath the LFS is the Physical File System (PFS). The PFS layer is where the distinction between files, sockets, and other resources is made. Based on the resource type, the LFS passes the incoming function requests to one of the following Physical File Systems:

Hierarchical file system PFS

This PFS handles requests related to resources in the z/OS UNIX Hierarchical File System (HFS).

AF_UNIX PFS

If a descriptor represents an AF_UNIX socket, the request is handled by this PFS. AF_UNIX sockets, often referred to as local sockets, enable two z/OS UNIX applications within the same system to communicate with each other.

AF_INET PFS

If a descriptor represents an AF_INET socket, it is handled by this PFS. AF_INET sockets are used on an IPv4 TCP/IP-based network and are commonly referred to as network sockets. If an IPv4 application wants to communicate with another program on a different TCP/IP host on an attached IP network, the application opens an AF_INET socket for that purpose.

AF_INET6 PFS

If a descriptor represents an AF_INET6 socket, it is handled by this PFS. AF_INET6 sockets are used on an IPv6 TCP/IP-based network and are commonly referred to as network sockets. If an IPv6 application wants to communicate with another program on a different TCP/IP host on an attached IP network, the application opens an AF_INET6 socket for that purpose.

From a TCP/IP perspective, the AF_INET and the AF_INET6 PFS are of main interest. TCP/IP is enabled for IPv6 by defining an AF_INET6 PFS. Defining the file systems is the responsibility of the installation's UNIX Systems Services

programmer. The definitions are found in the BPXPRMxx member of SYS1.PARMLIB. Refer to *z/OS Communications Server: IP Configuration Guide* for more information.

For a more detailed discussion of the Integrated and Common INET PFS, refer to *z/OS UNIX System Services Planning*.

The AF_INET and the AF_INET6 PFS can be configured two ways:

Integrated sockets PFS

The integrated sockets PFS can support the AF_INET PFS alone or AF_INET and AF_INET6 PFS together, but not AF_INET6 PFS alone.

Common INET PFS

This configuration is commonly referred to as the C_INET PFS configuration. It enables multiple AF_INET and AF_INET6 transport providers to be configured and active concurrently. Applications using the z/OS UNIX APIs do not know that multiple transport providers exist. For example, both the AnyNet[®] and TCP/IP Services components of z/OS V1R4 Communications Server can be configured at the same time. The AnyNet AF_INET PFS could provide access to an SNA network, while the TCP/IP AF_INET PFS could provide access to the TCP/IP network. The C_INET PFS is responsible for selecting the PFS over which to flow the request, based on the IP routing information from each of the AF_INET providers.

Under this configuration, it is also possible for TCP/IP application servers using the z/OS UNIX Socket APIs to field incoming client requests from all AF_INET transport providers without knowing the particular transport provider.

Application Programming Interfaces (APIs)

This section provides a short description of each of the programming interfaces that can be used to interface with the TCP/IP Services protocol stack provided by z/OS Communications Server. All of the APIs, with the exception of the PASCAL API, interface with the LFS layer previously described.

The APIs are divided into the following two categories:

- TCP/IP socket APIs provided by z/OS V1R4 Communications Server
- z/OS UNIX socket APIs

TCP/IP socket APIs provided by z/OS V1R4 Communications Server

z/OS V1R4 Communications Server provides six APIs to access TCP/IP sockets. These APIs can be used in either or both integrated and common INET PFS configurations. In a common INET PFS configuration, however, they function differently from z/OS UNIX-provided socket APIs. In this type of configuration, the z/OS Communications Server APIs always bind to a single PFS transport provider, and the transport provider must be the TCP/IP stack provided by z/OS V1R4 Communications Server.

The following TCP/IP socket APIs are included in z/OS V1R4 Communications Server:

Pascal API

The Pascal application programming interface enables you to develop TCP/IP applications in Pascal language. Supported environments are normal MVS address spaces. The Pascal programming interface is based

on Pascal procedures and functions that implement conceptually the same functions as the C socket interface. The Pascal routines, however, have different names than the C socket calls. Unlike the other APIs, the Pascal API does not interface directly with the LFS. It uses an internal interface to communicate with the TCP/IP protocol stack.

Pascal API only supports AF_INET.

CICS sockets

The CICS socket interface enables you to write CICS applications that act as clients or servers in a TCP/IP-based network. Applications can be written in C language, using the C sockets programming, or they can be written in COBOL, PL/I or assembler, using the Sockets Extended programming interface.

CICS sockets only support AF_INET.

C sockets

The C sockets interface supports socket function calls that can be invoked from C programs. However, note that for C application development, IBM recommends the use of the UNIX C sockets interface. These programs can be ported between MVS and most UNIX environments relatively easily if the program does not use any other MVS specific services.

C sockets only support AF_INET.

Sockets Extended macro API

The Sockets Extended macro API is a generalized assembler macro-based interface to sockets programming. It includes extensions to the socket programming interface, such as support for asynchronous processing on most sockets function calls.

The Sockets Extended macro API supports AF_INET and AF_INET6.

Sockets Extended Call Instruction API

The Sockets Extended Call Instruction API is a generalized call-based, high-level language interface to sockets programming. The functions implemented in this call interface resemble the C-sockets implementation, with some extensions similar to the sockets extended macro interface.

The Sockets Extended Call Instruction API supports AF_INET and AF_INET6.

REXX sockets

The REXX sockets programming interface implements facilities for socket communication directly from REXX programs by using an address rxsocket function. REXX socket programs can execute in TSO, online, or batch.

The REXX sockets programming interface supports AF_INET and AF_INET6.

Refer to *z/OS Communications Server: IP Application Programming Interface Guide* for complete documentation of the TCP/IP Services APIs.

z/OS UNIX APIs

The following APIs are provided by the z/OS UNIX element of z/OS and are supported by the TCP/IP stack in z/OS V1R4 Communications Server:

z/OS UNIX C sockets

z/OS UNIX C sockets is used in the z/OS UNIX environment. It is the z/OS UNIX version of the native MVS C sockets programming interface.

Programmers use this API to create applications that conform to the POSIX

or XPG4 standard (a UNIX specification). Applications built with z/OS UNIX C sockets can be ported to and from platforms that support these standards.

The z/OS UNIX C sockets support AF_INET and AF_INET6.

z/OS UNIX Assembler Callable Services

z/OS UNIX Assembler Callable Services is a generalized call-based, high-level language interface to z/OS UNIX sockets programming. The functions implemented in this call interface resemble the z/OS UNIX C sockets implementation, with some extensions similar to the sockets extended macro interface.

The z/OS UNIX Assembler Callable Services support AF_INET and AF_INET6.

Refer to *z/OS C/C++ Run-Time Library Reference* for complete documentation of the z/OS UNIX C sockets APIs and refer to *z/OS UNIX System Services Programming: Assembler Callable Services Reference* for information about z/OS UNIX Assembler Callable Services.

Applications

z/OS V1R4 Communications Server provides many applications that take advantage of TCP/IP protocols. Other applications, available from IBM or non-IBM vendors, can also be used with the z/OS V1R4 Communications Server product.

For descriptions of applications that have changed from previous releases, see these chapters:

- For a description of the FTP server and client, see Chapter 9, “Migrating the FTP server and client” on page 167.
- For a description of the z/OS Communications Server Telnet server and client, see Chapter 10, “Migrating the Telnet server and client” on page 203.
- For a description of the SNMP functions, see Chapter 11, “Migrating the SNMP server and client” on page 231.
- For a description of the BIND-based DNS name server, see Chapter 12, “Migrating to the BIND-based DNS name server” on page 249.
- For descriptions of other applications that are new or enhanced in z/OS V1R4 Communications Server, read the appropriate chapter or chapters listed below:
 - Chapter 4, “z/OS V1R4 Communications Server release summary” on page 65
 - Chapter 6, “z/OS V1R2 Communications Server release summary” on page 91
 - Chapter 8, “Communications Server for OS/390 V2R10 release summary” on page 135

For detailed information about configuration and operation of all z/OS V1R4 Communications Server applications, refer to *z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, *z/OS Communications Server: IP User's Guide and Commands*, *z/OS Communications Server: IP System Administrator's Commands*, and *z/OS Communications Server: IP Diagnosis*.

The applications included in z/OS V1R4 Communications Server can be grouped into the following categories:

- “System management applications” on page 9
- “Remote logon and file transfer applications” on page 11

- “Remote printing applications” on page 11
- “Remote execution applications” on page 12
- “Routing applications” on page 12
- “Mail facility applications” on page 13
- “Query resolution applications” on page 13
- “Network computing applications” on page 14
- “Miscellaneous applications” on page 15

Application tables

Each of the following sections contains a table indicating the particular release in which an application appeared as well as the subsequent releases for which the applications are supported. The tables do not indicate whether a particular application was enhanced from one release to another.

System management applications

The z/OS UNIX system management applications are invoked from the UNIX System Services environment.

Table 1 lists the system management applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 1. System management applications

Application	Releases
NETSTAT client	TSO NETSTAT supported in TCP/IP V3R1 and later; z/OS UNIX onetstat/netstat client supported in OS/390 V2R5 and later; MVS console D TCPIP,,NETSTAT client supported in OS/390 V2R5 and later
PING client	TSO PING supported in TCP/IP V3R1 and later; z/OS UNIX oping/ping client supported in OS/390 V2R5 and later
SNMP NetView® client	TCP/IP V3R1 and later
SNTP	z/OS CS V1R4
TRACERTE client	TSO client supported in TCP/IP V3R1 and later; z/OS UNIX otracert/traceroute client supported in OS/390 V2R5 and later
z/OS UNIX OMPROUTE SNMP subagent	OS/390 V2R7 and later
z/OS UNIX SNMP client	OS/390 V2R5 and later
z/OS UNIX SNMP server and subagent	OS/390 V2R5 and later
z/OS UNIX Policy Agent	OS/390 V2R7 and later
z/OS UNIX pasearch command	OS/390 V2R10 and later
z/OS UNIX RSVP Agent	OS/390 V2R8 and later
z/OS UNIX SLA Subagent	OS/390 V2R8 and later
z/OS UNIX trmdstat	OS/390 V2R10 and later
z/OS UNIX TRM daemon	OS/390 V2R10 and later
z/OS UNIX Trap Forwarder Daemon	OS/390 V2R10 and later

The following are brief descriptions of each system management application:

NETSTAT

Displays the network status of the local host, including information about TCP/IP connections, network clients, gateways, and devices. NETSTAT can also be used for diagnostic purposes.

PING (Packet Internet Groper)

Sends an Internet Control Message Protocol (ICMP) Echo Request to a gateway, router, or host with the expectation of receiving a reply.

Simple Network Time Protocol (SNTP)

Provides the time in order to synchronize a network of (S)NTP clients.

SNMP (Simple Network Management Protocol)

Monitors network elements attached to the TCP/IP internet.

TRACERTE

Displays the route that a packet takes to reach the requested target.

OMPROUTE SNMP Subagent

Supports the OSPF (Open Shortest Path First) MIB, which contains management data for OSPF routing protocol.

Policy Agent

Retrieves policy rules and actions from a policy configuration file and/or from a Lightweight Directory Access Protocol (LDAP) server and installs them in the z/OS Communications Server stack.

pasearch command

Displays detailed information for policy definitions that are managed by the Policy Agent.

RSVP Agent

Resource ReSerVation Protocol (RSVP) agent provides an API for applications to use in support of Integrated Services. (Integrated Services is a type of service that provides end-to-end Quality of Service (QoS) to an application, using the methodology of resource reservations along the data path from sender to receiver.)

SLA Subagent

SNMP SLA subagent supports the Service Level Agreement Performance Monitor (SLAPM) MIB. The SLA subagent allows network administrators to retrieve data and determine if the current set of SLA policy definitions are performing as needed or if adjustments need to be made.

trmdstat command

Generates reports based on Intrusion Detection Services (IDS) data extracted from the syslog daemon output. IDS includes TCP and UDP Traffic Regulation Management, Scan and Attack Detection.

TRM daemon

Collects and reports logging and statistics data for Intrusion Detection Services (IDS), which includes TCP and UDP Traffic Regulation Management, and Scan and Attack Detection.

Trap Forwarder Daemon

SNMP Trap Forwarder Daemon receives traps and forwards them to multiple other ports or addresses. It enables multiple z/OS SNMP managers to receive traps sent to one port.

Remote logon and file transfer applications

Table 2 lists the remote logon and file transfer applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 2. Remote logon and file transfer applications

Application	Releases
z/OS UNIX FTP server	App, OS/390 V2R5 and later
FTP client	TCP/IP V3R1 and later; z/OS UNIX FTP client supported in OS/390 V2R5 and later
TN3270 Telnet server	TCP/IP V3R1 and later
TN3270E Telnet server	OS/390 V2R5 and later
z/OS UNIX Telnet server	App, OS/390 V2R5 and later
TSO Telnet client	TCP/IP V3R1 and later

The following are brief descriptions of each remote logon and file transfer application:

FTP (File Transfer Protocol)

Allows you to transfer data sets and files between the local host and a remote host.

Telnet 3270 (TN3270) Server

Enables you to access Systems Network Architecture (SNA) applications from a remote Telnet 3270 client. This is a common way to access TSO/VTAM remotely.

z/OS UNIX Telnet Server

Allows you to access the UNIX system services shell from a remote Telnet client.

TSO Telnet Client

Allows you to connect to remote Telnet 3270 servers or UNIX Telnet servers. UNIX Telnet is supported in line mode only.

Remote printing applications

Table 3 lists the remote printing applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 3. Remote printing applications

Application	Releases
LPD daemon	TCP/IP V3R1 and later
LPR client	TCP/IP V3R1 and later
NPF server	TCP/IP V3R1 and later

The following are brief descriptions of each remote printing application:

LPD (Line Printer Daemon)

Defines and controls printers that may be local or remote. Local printers may be attached to the MVS spooling system.

LPR (Line Printer Requester)

Sends a file to a printer controlled by the line printer daemon on the local host or a remote host.

NPF (Network Print Facility)

Redirects output from LU0, LU1, LU3, or JES managed printers to printers on any TCP/IP host.

Remote execution applications

Table 4 lists the remote execution applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 4. Remote execution applications

Application	Releases
TSO REXEC client	TCP/IP V3R1 and later
z/OS UNIX REXEC client	App, OS/390 V2R5 and later
REXECD/RSHD server	TCP/IP V3R1 and later
z/OS UNIX REXECD server	App, OS/390 V2R5 and later
TSO RSH client	TCP/IP V3R1 and later
z/OS UNIX RSHD server	App, OS/390 V2R5 and later

The following are brief descriptions of each remote execution application:

REXEC

Executes commands on a remote system and receives the results on the local host.

REXECD/RSHD

REXECD provides server functions for remote commands based on the Remote Execution (REXEC) protocol. RSHD provides server functions for remote shell clients based on the Remote Shell (RSH) protocol.

RSH

Executes commands on a remote file system and receives the results on the local host. The RSH client is similar to REXEC.

Routing applications

Table 5 lists the routing applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 5. Routing applications

Application	Releases
NCROUTE server	TCP/IP V3R1 and later
OMROUTE daemon	OS/390 V2R6 and later
OROUTED daemon	OS/390 V2R4 and later

The following are brief descriptions of each routing application:

NCROUTE

Provides dynamic routing for an IP router that is part of a network control program (ACF/NCP)

OMROUTE

Dynamically updates routing tables using the Open Shortest Path First (OSPF) Protocol and Routing Information Protocol (RIP).

OROUTED

Dynamically updates routing tables using RIP protocols.

Mail facility applications

Table 6 lists the mail applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 6. Mail facility applications

Application	Releases
z/OS UNIX popper	OS/390 V2R6 and later
z/OS UNIX sendmail agent/server	OS/390 V2R6 and later
SMTP server	TCP/IP V3R1 and later

The following are brief descriptions of each mail facility application:

popper

Accesses the mail spool file on a local host.

sendmail

Transfers mail among users in the z/OS UNIX environment.

SMTP (Simple Mail Transfer Protocol)

Transfers mail among users in the Internet environment by specifying the mail exchange sequences and message format.

Query resolution applications

Table 7 lists the query resolution applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 7. Query resolution applications

Applications	Releases
DNS name server Version 4; also called z/OS UNIX DNS name server (BIND-based)	OS/390 V2R5 and later
DNS name server Version 9	z/OS CS V1R2 and later
PORTMAPPER server	TCP/IP V3R1 and later
NSLOOKUP client	TCP/IP V3R1 and later
z/OS UNIX DIG client	z/OS CS V1R2 and later
z/OS UNIX dnsdomainname	OS/390 V2R8 and later
z/OS UNIX domainname	OS/390 V2R8 and later
z/OS UNIX host	OS/390 V2R8 and later
z/OS UNIX hostname	OS/390 V2R8 and later
z/OS UNIX nslookup client	OS/390 V2R5 and later. In z/OS CS V1R2, it has new options in BIND.9 mode.
z/OS UNIX nsupdate client	OS/390 V2R5 and later. In z/OS CS V1R2, it has new options in BIND.9 mode.
z/OS UNIX portmapper server	App, OS/390 V2R5 and later
TSO DIG client	TCP/IP V3R1 and later

The following are brief descriptions of each query resolution application:

DNS (Domain Name System) name server

Provides host name-to-IP address mappings in a network.

PORTMAPPER

Maps Open Network Computing/Remote Procedure Call (ONC/RPC) application client programs to the port numbers of server programs.

nslookup

Queries a name server.

DIG The domain information groper (dig) is a command line tool that can be used to gather information from the Domain Name System servers. In z/OS CS V1R2 and later, it can be run from the UNIX shell. It has different options than the previous TSO DIG command.

dnsdomainname

UNIX command that displays the DNS domain name of the local host.

domainname

Like dnsdomainname, domainname is UNIX command that displays the DNS domain name of the local host.

host UNIX command that converts between IP addresses and host names.

hostname

UNIX command that displays the host name of the local host.

nsupdate

Provides a command line interface for generating dynamic DNS update requests and generates keys for dynamic DNS update requests.

Network computing applications

Table 8 lists the network computing applications in z/OS Communications Server and indicates the releases for which the applications are supported.

Table 8. Network computing applications

Applications	Releases
TFTP	OS/390 V2R5 and later
DHCP	OS/390 V2R5 and V2R6 only
DHCP/PXE	OS/390 V2R7 and later
TIMED	OS/390 V2R5 and later
BINL	OS/390 V2R7 and later
SNTP server	z/OS CS V1R4 and later

The following are brief descriptions of each network computing application:

TFTP (Trivial File Transfer Protocol)

Provides simple file retrieval with limited security.

DHCP (Dynamic Host Configuration Protocol)

Provides dynamic IP address information to clients.

DHCP/PXE (Dynamic Host Configuration Protocol/Preboot Execution Environment)

Performs normal DHCP operations, Preboot Execution Environment (PXE) proxy operations, or both.

TIMED (Time Daemon)

Provides clients with Universal Time Code (UTC) time. Network stations without a time chip obtain clocks from this daemon.

BINL (Bind Image Negotiation Layer) server

Works interactively with the DCHP/PXE server to enable a client to identify the name of a boot file and the IP address of the boot server.

SNTP (Simple Network Time Protocol) server

Provides the time in order to synchronize a network of (S)NTP clients.

Miscellaneous applications

Table 9 shows another application available in z/OS Communications Server and indicates the releases for which the application is supported.

Table 9. Miscellaneous application

Applications	Releases
MISCSERV server	TCP/IP V3R1 and later

The MISCSERV server is used to test and debug applications and networks. MISCSERV supports the ECHO, DISCARD, and CHARGEN protocols.

Programming tools and libraries

Table 10 shows the tools and libraries available in z/OS Communications Server and indicates the releases for which the tools and libraries are supported.

Table 10. Programming tools and libraries

Tools and libraries	Releases
NCS	TCP/IP V3R1 and later
NDB	TCP/IP V3R1 and later
ONC/RPC libraries	App, OS/390 V2R5 and later
OSF/Motif and X Window System for TSO	TCP/IP V3R1 and later
OS/390 UNIX OSF/Motif and X-Window System	App, OS/390 V2R5 and later
SNMP DPI [®] version 1.1	TCP/IP V3R1 and later
SNMP DPI version 2.0	App, OS/390 V2R5 and later
RSVP API (RAPI)	OS/390 V2R8 and later

The following are brief descriptions of these tools and libraries:

NCS (Network Computing System)

Set of software tools, developed by Apollo Computer, Inc., that conform to the Network Computing Architecture. These tools include the remote procedure call run-time library, the Location Broker, and the NIDL compiler.

NDB (Network Database)

DB2[®] information with a wide range of supported Structured Query Language (SQL) processing. With NDB, you can develop client and server applications that retrieve and update information stored in the DB2 maintained databases.

ONC/RPC (Open Network Computing/Remote Procedure Call)

Application programming interface used for remote procedure call server and client applications in z/OS UNIX.

OSF/Motif and X Window System

X Window System-based widget set.

DPI (Distributed Programming Interface)

Provides routines for writing SNMP subagents.

RSVP API (RAPI)

An application programming interface (API) for the Resource ReSerVation Protocol (RSVP), known as RAPI, that is included in the z/OS UNIX RSVP Agent. The RAPI interface is a set of C language bindings that provides client library calls. Refer to *z/OS Communications Server: IP Programmer's Reference* for detailed information.

TCP/IP packaging process

As a result of the installation process for z/OS V1R4 Communications Server, the product is now installed in both traditional MVS data sets and in files in the z/OS UNIX HFS. For details on changes in the MVS data sets, see “MVS data sets”. For details on requirements for HFS files, see “HFS files” on page 18.

MVS data sets

Table 11 lists the distribution library data sets required by z/OS V1R4 Communications Server.

Table 11. Distribution library data sets

Data set	Description
AEZADBR1	Database Request Module (DBRM) members
AHELP	TSO help files
AEZAMAC1	Assembler macros
AEZAMAC2	C header files
AEZAMAC3	Pascal includes
AEZAMODS	Distribution library for base link-edit modules
AEZARNT1	Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS
AEZARNT4	Reentrant object modules for RPC
AEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)
AEZASMP1	Sample source programs, catalog procedures, CLIST, and installation jobs
AEZAXLTD	Translated default tables
AEZAXLTK	Translated Kanji, Hangeul, and Traditional Chinese DBCS tables and codefiles
AEZAXLT1	Translation table SBCS source and DBCS source for Hangeul and Traditional Chinese
AEZAXLT2	TELNET client translation tables
AEZAXLT3	Kanji DBCS translation table source
ABLSCLI0	clists, execs
ABLMSG0	messages
ABLSPNL0	panels
ABLSTBL0	tables

Table 12 lists the target library data sets required by z/OS V1R4 Communications Server.

Table 12. Target library data sets

Data set	Description
SEZACMAC	Client Pascal macros, C headers, and assembler macros
SEZACMTX	Load library for linking user modules and programs
SEZADBCX	Source for the Kanji, Hangeul, and Traditional Chinese DBCS translation tables
SEZADBRM	DBRM members
SEZADPIL	SNMP Distributed Programming Interface library
SEZADSIL	SNMP command processor and SNMPIOCV subtask for the NetView program, and the SQESERV module for the SNMP query engine
SEZADSIM	SNMP messages for the NetView program
SEZADSIP	SNMPIOCV initialization parameters for the Netview program
HELP	TSO help files
SEZAINST	Installation samples and related members
SEZALIBN	NCS library system library
SEZALOAD	Executable load modules for concatenation to LINKLIB
SEZALNK2	LB@ADMIN for the NCS administrator
SEZALPA	Executable load modules for concatenation to LPALIB
SEZAMENU	Messages for the Network Print Facility and IPCS
SEZANCLS	SNMP CLISTS
SEZANMAC	C headers and assembler macros for z/OS UNIX and TCP/IP Services APIs
SEZANPNL	SNMP panels
SEZAPENU	ISPF panels for the Network Print Facility and IPCS
SEZARNT1	Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS
SEZARNT4	Reentrant object modules for RPC
SEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)
SEZARPCL	Remote procedure call library
SEZATCP	Executable load modules for STEPLIB or LINKLIB concatenation
SEZATCPX	Source for the country SBCS translation tables
SEZATELX	Source for the TELNET country translation tables
SEZAXLD1	Translated default tables
SEZAXLD2	Translated Kanji, Hangeul, and Traditional Chinese DBCS default tables and DBCS codefiles for TELNET transform mode

Table 13 lists the shared distribution and target library data sets required by z/OS V1R4 Communications Server.

Table 13. Shared distribution and target library data sets

Data set	Description
MIGLIB	Load modules that are used from another system for migration purposes and IPCS load modules
MSGENU / AMSGENU	English-language message tables used by the MVS message service (MMS)
NUCLEUS	Resident SVCs, callable services tables, and abnormal termination modules
PARMLIB / APARMLIB	IBM-supplied and installation-created members, which contain lists of system parameter values
SBLSCLI0	Contains CLISTs and REXX execs 7
SBLSMSGS	Contains messages
SBLSPNL0	Dialog panels for the interactive problem control system (IPCS) dialog programs
SBLSTBL0	Contains tables, keys, and commands
SCIMXML / ACIMPLUG	Managed System Infrastructure Product Definition XML

HFS files

For a description of the Hierarchical File System (HFS) files, refer to *z/OS UNIX System Services Planning* and *z/OS UNIX System Services User's Guide*.

z/OS Communications Server HFS parts

Table 14 shows the location of the z/OS V1R4 Communications Server HFS parts. Executables marked with the number 1 exist only in the HFS with the sticky bit off. All the remaining executables exist only in an MVS data set. The HFS contains a nonexecutable module with the sticky bit on. If the sticky bit is on, these modules are fetched from z/OS Communications Server MVS library data sets (for example, TCPIP.SEZALOAD).

Table 14. Location of z/OS Communications Server HFS parts

Function	HFS file	MVS data set
FTP client	/bin/ftp	SEZALOAD
UNIX pasearch command	/bin/pasearch (1)	n/a
UNIX trmdstat command	/bin/trmdstat (1)	n/a
UNIX netstat client	/bin/onetstat and /bin/netstat	SEZALOAD
UNIX ping client	/bin/oping and /bin/ping	SEZALOAD
UNIX REXEC client	/bin/orexec and /bin/rexec	SEZALOAD
UNIX SNMP client	/bin/osnmp and /bin/snmp	SEZALOAD
UNIX Traceroute	/bin/otracer and /bin/traceroute	SEZALOAD
UNIX SNMP pwtokey	/bin/pwtokey	SEZALOAD
UNIX SNMP pwchange	/bin/pwchange	SEZALOAD
UNIX host command	/bin/host (1)	n/a
UNIX hostname command	/bin/hostname (1)	n/a
UNIX dnsdomainname command	/bin/dnsdomainname (1)	n/a
UNIX domainname command	/bin/domainname (1)	n/a
IOCTL DVIPA Creation Utility	/bin/moddvipa	SEZALOAD

Table 14. Location of z/OS Communications Server HFS parts (continued)

Function	HFS file	MVS data set
z/OS UNIX REXECD server	/usr/sbin/orexecd	SEZALOAD
z/OS UNIX OROUTED server	/usr/sbin/orouted	SEZALOAD
z/OS UNIX OMPROUTE server	/usr/sbin/omproute	SEZALOAD
z/OS UNIX RSHD server	/usr/sbin/orshd	SEZALOAD
z/OS UNIX SNMP server	/usr/sbin/osnmpd	SEZALOAD
z/OS UNIX TELNETD server	/usr/sbin/otelnetd	SEZALOAD
z/OS UNIX sendmail server	/usr/sbin/sendmail (1)	n/a
z/OS UNIX mailstats server	/usr/sbin/mailstats (1)	n/a
z/OS UNIX popper client	/usr/sbin/popper	SEZALOAD
Syslogd server	/usr/sbin/syslogd	SEZALOAD
z/OS UNIX Policy agent server	/usr/sbin/pagent	SEZALOAD
z/OS UNIX SLA subagent	/usr/sbin/pagtsnmp	SEZALOAD
z/OS UNIX RSVP agent	/usr/sbin/rsvpd	SEZALOAD
z/OS UNIX trap forwarder daemon	/usr/sbin/trapfwd	SEZALOAD
z/OS UNIX traffic regulation management daemon	/usr/sbin/trmd	SEZALOAD
Digital Certificate Access Server (DCAS)	/usr/sbin/dcas	SEZALOAD
Network Computing Applications		
DHCP Admin interface server	/usr/sbin/dadmin	SEZALOAD
DHCP server	/usr/sbin/dhcpsd	SEZALOAD
BINL server	/usr/sbin/binlsd	SEZALOAD
Trivial FTP server	/usr/sbin/tftpd	SEZALOAD
TIMED server	/usr/sbin/timed	SEZALOAD
SNTPD	/usr/sbin/sntpd	SEZALOAD
z/OS UNIX FTPD server		
Listener	/usr/sbin/ftpd	SEZALOAD
Server	/usr/sbin/ftpdns	SEZALOAD
z/OS UNIX ONC/RPC		
Portmapper command	/bin/oportmap and /bin/portmap	SEZALOAD
ONC RPC protocol compiler	/bin/orpcgen and /bin/rpcgen	SEZALOAD
RPCINFO command	/bin/orpcinfo and /bin/rpcinfo	SEZALOAD
Header files	/usr/include/rpc	n/a
Library archive	/usr/lib/librplib.a	n/a
Sample code	/usr/lpp/tcpip/rpc/samples	n/a
BIND-based DNS		

Table 14. Location of z/OS Communications Server HFS parts (continued)

Function	HFS file	MVS data set
nsupdate client	/bin/nsupdate (1) /bin/nsupdat4	n/a SEZALOAD
onslookup client	/bin/onslookup (1) and /bin/nslookup and /bin/nslookup4 (1)	n/a n/a
named server	/usr/sbin/named and /usr/sbin/named4	SEZALOAD
namedxfr	/usr/sbin/namedxfr	SEZALOAD
dig client	/bin/dig (1)	n/a
dnsmigrate	/bin/dnsmigrate (1)	n/a
dnssec-keygen	/bin/dnssec-keygen (1)	n/a
dnssec-makekeyset	/bin/dnssec-makekeyset (1)	n/a
dnssec-signkey	/bin/dnssec-signkey (1)	n/a
dnssec-signzone	/bin/dnssec-signzone (1)	n/a
rndc	/bin/rndc (1)	n/a
Managed System Infrastructure (mSys)		
mSys host plug-in	/usr/lpp/cim/plugin/ezacim.jar	n/a
mSys workplace plug-in	/usr/lpp/cim/plugin/ezacimx.jar	n/a
X Window System		
Header files	/usr/include	n/a
Library archives	/usr/lib	n/a
Uil Compiler	/bin/X11/uil (1)	n/a
Sample code	/usr/lpp/tcpip/X11R6/Xamples	n/a

Refer to *z/OS Communications Server: IP Configuration Reference* for a list of HFS files with definitions.

Encryption features

Encryption features are available at no additional cost, but must be ordered separately from the z/OS base. Level 3 is the only level available for ordering with z/OS V1R4 Communications Server. Effective with z/OS V1R2 Communications Server, Kerberos support is no longer provided by Communications Server. For the z/OS platform, Kerberos support is provided through the z/OS Security Server. If you were using the Kerberos support provided by Communications Server, you must now use the Security Server Kerberos support. Please refer to *z/OS Security Server Network Authentication Service Administration* and *z/OS Security Server Network Authentication Service Programming* for more information.

The encryption features include the following capabilities:

Level 1

This level of encryption is included in the base of z/OS V1R4 Communications Server.

Level 2

This level of encryption is included in the base of z/OS V1R4 Communications Server and offers IP Security (IPSec) DES/CDMF and SNMPv3 56 bit DES.

|
|
|

Level 3

This level of encryption is shipped, if ordered, as FMID JIP614K and offers IPSec Triple DES.

Chapter 2. Migration overview

This chapter includes the following:

- A table designed to be used as a roadmap to IP functions and enhancements that were introduced in CS for OS/390 V2R10, z/OS CS V1R2, and z/OS CS V1R4. The **Enabling / migration actions** column indicates if tasks are required to either utilize the functional enhancement or to satisfy incompatibilities or dependencies. The **Reference** column points you to the section of this document that describes the enhancement and the migration tasks.
- A planning and migration checklist.

Table 15. Migration roadmap

Functional enhancement	Enabling / migration actions	Reference
Enhancements introduced in z/OS CS V1R4		
Sysplex-wide Dynamic Source VIPAs for TCP connections	Yes	Page 66
Sysplexports	Yes	Page 67
Sysplex Wide Security Association (SWSA)	Yes	Page 68
Network access control	Yes	Page 69
Fast Response Cache Accelerator (FRCA) access control	Yes	Page 70
Resolver enhancements (general enhancement — see page 82 for resolver enhancements related to IPv6 support)	Yes	Page 70
Managed System Infrastructure (msys) for Setup enhancement	Yes	Page 71
OSA SNMP subagent support	No	Page 72
Event trace enhancements	Yes	Page 72
TCP/IP support for Simple Network Time Protocol (SNTP)	Yes	Page 73
Netstat enhancements (general enhancement — see page 84 for Netstat enhancements related to IPv6 support)	No	Page 74
Ping enhancements (general enhancement — see page 85 for Ping enhancements related to IPv6 support)	Yes	Page 74
Traceroute enhancements (general enhancement — see page 85 for Traceroute enhancements related to IPv6 support)	Yes	Page 74
New VTAM start options to adjust the QDIO or iQDIO storage	Yes	Page 78
Enabling IPv6 support	Yes	Page 79
Configuration changes related to IPv6 support	Yes	Page 80
IPv6 support for the resolver	Yes	Page 82
IPv6 support for applications	Yes	Page 83
IPv6 support for Netstat	Yes	Page 84
IPv6 support for Ping	Yes	Page 85
IPv6 support for Traceroute	Yes	Page 85

Table 15. Migration roadmap (continued)

Functional enhancement	Enabling / migration actions	Reference
IPv6 support for IPv6 IPCS subcommands formatting	No	Page 86
IPv6 support for event trace enhancements	Yes	Page 86
IPv6 support for RAS packet trace and data trace	No	Page 87
IPv6 support for socket API commands	Yes	Page 87
FTP support for substitution characters during EBCDIC/ASCII single-byte translations	Yes	Page 175
FTP: Enhanced FTP activity logging	Yes	Page 176
FTP: Changed behavior of login failure replies	No	Page 176
FTP: Support for Chinese standard GB18030 provided by codepage IBM-5488	Yes	Page 177
FTP: Enhancements to FTP server user exits	Yes	Page 178
FTP: IPv6 support for FTP	Yes	Page 180
Telnet: Port qualification by linkname or destination IP address	Yes	Page 211
Telnet: Printer enhancements	Yes	Page 212
Telnet: Parameter placement enhancements	No	Page 213
Telnet: New DEBUG option to suppress the connection dropped error messages	Yes	Page 213
Telnet: New QINIT option for default applications	Yes	Page 214
Telnet: LU mapping enhancements	Yes	Page 214
Upgrade TN3270 SSL to use TLS	No	Page 215
DNS enhancements, including IPv6 support	Yes	Page 252
Enhancements introduced in z/OS CS V1R2		
Resolver enhancements	Yes	Page 92
Intrusion Detection Services (includes TRM enhancements)	Yes	Page 95
Sysplex Distributor policy enhancements	Yes	Page 98
Policy Agent enhancements	Yes	Page 100
OROUTED to OMPROUTE migration	Yes	Page 102
OMPROUTE to allow RIP1 and RIP2 packets over the same interface	Yes	Page 103
Replaceable static routes	Yes	Page 104
OMPROUTE wildcard IP addressing enhancement	Yes	Page 105
Additional RIP filter for OMPROUTE	Yes	Page 106
OSPF MD5 authentication	Yes	Page 106
Native Socket API TCP_NODELAY support	Yes	Page 108
Netstat filter enhancements	No	Page 109
Netstat performance counters	No	Page 109
Restrict access to netstat commands	Yes	Page 110
z/OS UNIX RSHD Kerberos support	Yes	Page 111
Application-driven policy classification	Yes	Page 112
Virtual LAN priority tagging	Yes	Page 112

Table 15. Migration roadmap (continued)

Functional enhancement	Enabling / migration actions	Reference
Packet trace enhancements	No	Page 113
Fast connection reset for Sysplex Distributor	No	Page 114
HiperSockets	Yes	Page 114
Efficient routing using HiperSockets Accelerator	Yes	Page 117
Connection load balancing using Sysplex Distributor in a network with Cisco routers	Yes	Page 118
CICS sockets listener enhancements	Yes	Page 120
SMF recording enhancements	Yes	Page 121
SMTP exit to filter unwanted mail	Yes	Page 122
Managed System Infrastructure (msys) for Setup	Yes	Page 123
Improve TCP/IP storage utilization management	Yes	Page 124
Enterprise Extender performance enhancements	No	Page 125
Enhanced CLAW packing	Yes	Page 125
64-bit real addressing support	No	Page 126
OSA-Express token ring support	No	Page 127
Changes to EZAZSSI	No	Page 129
IPSec enhancements	No	Page 130
TCP configuration options	Yes	Page 130
Enhancing FTP server security	Yes	Page 181
FTP Restrict DIR output	No	Page 182
FTP Surrogate RACF support	Yes	Page 183
Socksify FTP client	Yes	Page 183
TLS enablement for FTP	Yes	Page 184
Kerberos support for the FTP server and client	Yes	Page 185
FTP ISPF statistics	Yes	Page 186
User-level FTP server options	Yes	Page 187
FTP Stream mode restart	Yes	Page 187
FTP RFC updates	Yes	Page 188
FTP Native ASCII support	Yes	Page 190
FTP trace enhancements	Yes	Page 191
z/OS UNIX Telnet (otelnetd) server – Kerberos support	Yes	Page 216
TN3270 diagnostics enhancements	Yes	Page 217
TN3270E RFC 2355 SNA extensions	Yes	Page 218
TN3270 profile and display enhancements	Yes	Page 218
Express Logon Feature using TN3270E Server on z/OS	Yes	Page 221
SNMP security enhancements	Yes	Page 237
SNMP Community MIB	Yes	Page 237
SNMP Dynamic VIPA MIB enhancements	Yes	Page 239
SNMP OSA-Express MIB enhancements	Yes	Page 239
SNMP TCP/IP performance counters	Yes	Page 239

Table 15. Migration roadmap (continued)

Functional enhancement	Enabling / migration actions	Reference
BIND DNS upgrade	Yes	Page 256
Enhancements introduced in CS for OS/390 V2R10		
Sysplex Distributor	Yes	Page 135
Non-disruptive VIPA takeover	Yes	Page 138
Policy Agent enhancements	Yes	Page 139
Service Level Policy Quality of Service (QoS) enhancements	Yes	Page 141
Traffic Regulation and Management (TRM)	Yes	Page 142
Queued Direct I/O (QDIO) queue management for MPCIPA devices	No	Page 143
MPCIPA Queued Direct I/O enhancements for Fast Ethernet and ATM LAN-Emulation	Yes	Page 144
MPCIPA Queued Direct I/O Address Resolution Protocol (ARP) cache enhancements	Yes	Page 146
syslogd isolation	Yes	Page 146
Port access control	Yes	Page 148
Stack access control	Yes	Page 149
Network access control	Yes	Page 150
Server bind control	Yes	Page 151
On-demand tunnels	No	Page 152
REXEC enhancements	Yes	Page 153
IPv6 API	Yes	Page 153
Express Logon feature: Digital Certificate Access Server (DCAS)	Yes	Page 155
TCP/IP IPCS command enhancements	Yes	Page 158
Socket API trace	Yes	Page 159
TCP/IP trace enhancements	Yes	Page 160
Fast Local Sockets	Yes	Page 160
Fast Response Cache Accelerator (FRCA) enhancement	Yes	Page 161
IP Security (IPSec)	No	Page 162
Route lookup improvements	Yes	Page 162
CDLC device driver support for greater than 4K MTU	Yes	Page 163
CLAW packing within a 4K frame	Yes	Page 164
FTP server usability enhancements	Yes	Page 192
FTP server administration enhancements	Yes	Page 193
FTP server functional and compatibility enhancements	Yes	Page 196
FTP server user exit enhancements	Yes	Page 200
FTP client usability enhancements	Yes	Page 201
FTP client administration enhancements	Yes	Page 201
FTP client functional and compatibility enhancements	Yes	Page 201
TN3270 SSL enhancement	Yes	Page 223

Table 15. Migration roadmap (continued)

Functional enhancement	Enabling / migration actions	Reference
TN3270 System SSL	Yes	Page 224
TN3270 enhanced SLU simulation	Yes	Page 225
TN3270 NQN enhancement for the TN3270E server	Yes	Page 226
TN3270 client reconnect to TN3270E server	Yes	Page 226
TN3270E resource pooling	Yes	Page 227
TN3270 Timemark default change	Yes	Page 228
SNMPv3 enhancements	Yes	Page 240
SNMP Allow source VIPA	Yes	Page 243
SNMP TCP/IP subagent	Yes	Page 243
SNMP Trap-Forwarder Daemon	Yes	Page 248
DNS SRV Resource Record support	Yes	Page 262
DNS non-swappable mode support	Yes	Page 263

Planning and migration checklist

Migrating a TCP/IP system from a previous release involves considerable planning. To familiarize yourself with the migration process, review the checklist below. Tailor the checklist to meet the specific requirements of your installation.

1. Understand your network topology.
 - Understand the hardware and software you have in your network and your network configuration.
2. z/OS V1R4 Communications Server is a base element of z/OS. The functional enhancements are described in the release summary chapters. z/OS CS hardware, network, and software requirements are described in *z/OS and z/OS.e Planning for Installation*. For information about storage requirements, refer to the *z/OS Program Directory* and the appropriate INFOAPAR on RETAIN (see Appendix C, “Information APARs” on page 279 for the APAR numbers).
3. Develop your education plan:
 - Evaluate the z/OS V1R4 Communications Server features and enhancements. Plan which new functions will be incorporated into your system.
 - Order the appropriate publications.
4. Review and apply the Program Temporary Fixes (PTFs), including Recommended Service Upgrades (RSUs), for the current-minus-3 month plus all hipers and PEs. The PTFs are available monthly through the period for which the release is current and can be obtained by using IBMLINK. RSU integration testing for a release will be performed for five quarters after the general availability date for that release.
5. Review the appropriate installation information:
 - *z/OS Program Directory*
 - Preventative Service Planning (PSP) bucket (available by using IBMLINK)
 - Softcopy Installation Memo (for Bookmanager publications)
 - *ServerPac: Installing Your Order*, if you use the ServerPac method to install z/OS

- |
- |
6. Read the hints, tips, and so on found at website www-4.ibm.com/software/network/commsserver/support.
 7. Plan what has to be done to apply new functions to your system.
 8. In writing a test plan for z/OS, include test cases for the following:
 - TCP/IP applications
 - User-written applications such as the following: Customer Information Control System (CICS) sockets, Information Management System (IMS) sockets, REXX sockets, Sockets Extended, UNIX System Services sockets, and Macro Sockets
 - Operator commands
 - Your terminal and printer types
 9. Back up your user exits and user modifications for later restore.
 10. Install TCP/IP with the other elements and features of z/OS. IBM has defined the appropriate product enablement settings in the IFAPRD00 member of SYS1.IBM.PARMLIB. For information about dynamic enablement, refer to *z/OS and z/OS.e Planning for Installation*.
 11. Complete post-installation activities:
 - Use the *z/OS Communications Server: IP Configuration Guide* to customize your TCP/IP system.
 - Reinstall user exits.
 - Reinstall user modifications.
 - Update operating procedures and automation routines.
 - Activate new functions.
 12. Complete functional and stress tests.

Chapter 3. New and changed interfaces

This chapter consists of tables that describe updates to configuration files, commands, environment variables, socket APIs, and other APIs. The tables are intended to help you migrate by identifying what is new or changed since your last installation. See “z/OS Communications Server information” on page xxiii to determine which publications you should refer to for complete information about the interfaces, including syntax.

The updates shown in the following tables were made in CS for OS/390 V2R10 or later:

- Configuration files (other than PROFILE.TCPIP), Table 16
- TCPIP.DATA, Table 17 on page 31
- PROFILE.TCPIP configuration file, Table 18 on page 31
- SYS1.PARMLIB members, Table 19 on page 35
- Operator commands, Table 20 on page 36
- TSO commands, Table 21 on page 43
- UNIX commands, Table 22 on page 49
- Environment variables, Table 23 on page 58
- TCP/IP socket API commands enabled for IPv6, Table 24 on page 58
- TCP/IP socket APIs, Table 25 on page 59
- “IPCS subcommands” on page 61

Refer to Chapter 3, “New and Changed Interfaces” in *z/OS IBM Communications Server: IP Migration Version 1 Release 2* to see interface updates made prior to CS for OS/390 V2R10. You may access this document at the following URL:
<http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>.

Changes to FTP, Telnet, SNMP and the BIND-based DNS name server are described in their respective chapters in this document. They are not included here.

Configuration files

Table 16. New or changed configuration files

File	Statement or parm	Description	Status
OMPROUTE configuration file		File used to configure OMPROUTE.	
	OSPF_INTERFACE	Parameter (AUTHENTICATION_TYPE) to control authentication type by interface.	New in z/OS CS V1R2
		Parameter (AUTHENTICATION_KEY_ID) used with MD5 authentication to specify the MD5 key ID.	New in z/OS CS V1R2
		Parameter (AUTHENTICATION_KEY) upgraded to allow specification of MD5 keys	Changed in z/OS CS V1R2
RIP_INTERFACE	RECEIVE_RIP has new values to independently control sending and receiving RIP1 and RIP2 packets	Changed in z/OS CS V1R2	

Table 16. New or changed configuration files (continued)

File	Statement or parm	Description	Status	
Policy Agent configuration file		File used to configure the Policy Agent.		
	LogLevel	Specifies desired level of logging. Default loglevel changed from 15 to 31.	Changed in z/OS CS V1R2	
	PolicyAction	Defines Version 2 (V2R10) policy actions: <ul style="list-style-type: none"> • Allows definition of differentiated services policy values • Allows a new policy scope, TR, for traffic regulation policies, as well as traffic regulation actions and limits 	New in CS for OS/390 V2R10	
	PolicyPerfMonitorForSDR	Added to enable or disable the policy performance monitor function that assigns a weight fraction to the monitored policy performance data and sends messages to the Sysplex Distributor Routing (SDR) component as the monitored data crosses its defined thresholds.	New in CS for OS/390 V2R10	
	PolicyRule		Defines Version 2 (V2R10) policy rules and supports better policy activation criteria and traffic filtering.	New in CS for OS/390 V2R10
			Parameter added to identify rules for the Sysplex Distributor distributing stack.	Changed in z/OS CS V1R2
	ReadFromDirectory		Enhanced to allow specification of a backup LDAP server and port, the LDAP protocol version and schema version, search criteria, and LDAP server SSL connection information	Changed in CS for OS/390 V2R10
		Enhanced with new parameters to assist with retrieving schema version 3 objects from an LDAP server.	Changed in z/OS CS V1R2	
Policy Agent configuration file (continued)	TcpImage	Specifies stack-specific parameters for installing service policies. PURGE option added in z/OS V1R2 to purge all policies from the stack.	Changed in z/OS CS V1R2	
	SetSubnetPrioTosMask	Defines the mapping of Type of Service (ToS) byte to device priorities. PriorityTosMapping parameter is enhanced to also allow mapping of TOS byte to Virtual LAN (VLAN) user priority.	Changed in z/OS CS V1R2	
Resolver setup file		File used to configure resolver.	New in z/OS CS V1R2	
	GLOBALTCPIPDATA and DEFAULTTCPIPDATA	Resolver setup statements	New in z/OS CS V1R2	
	GLOBALIPNODES, DEFAULTIPNODES and COMMONSEARCH / NOCOMMONSEARCH	Resolver setup statements	New in z/OS CS V1R4	

Table 16. New or changed configuration files (continued)

File	Statement or parm	Description	Status
SYSLOGD configuration file		SYSLOGD records can now be written to SMF.	Changed in CS for OS/390 V2R10

TCPIP.DATA

Table 17. New or changed TCPIP.DATA statements and parameters

Statement or parm	Description	Status
DOMAIN	This is functionally equivalent to the DOMAINORIGIN statement.	New in z/OS CS V1R2
LOOKUP	Specifies the order in which the DNS or local host files should be used to satisfy name or address resolution requests.	New in z/OS CS V1R2
NAMESERVER	This is functionally equivalent to the NSINTERADDR statement.	New in z/OS CS V1R2
OPTIONS	Specifies the following: <ul style="list-style-type: none"> If resolver debug messages should be issued The number of periods that need to be contained in a domain name for it to be considered a fully qualified domain name 	New in z/OS CS V1R2
SEARCH	Specifies the list of domain names that are appended, in the order listed, to the host name to form the fully qualified domain name for a host.	New in z/OS CS V1R2
SORTLIST	Specifies the ordered list of network numbers (subnets or networks) for the resolver to prefer if it receives multiple addresses as the result of a name query.	New in z/OS CS V1R2

PROFILE.TCPIP configuration file

Table 18. New or changed PROFILE.TCPIP configuration statements and parameters

Statement or parm	Description	Status
ATMLIS	BEARERCLASS option added where class can be either A, C, or X.	Changed in z/OS CS V1R2
BEGINROUTES / ENDROUTES	Statement block to define static routes to the IP route table. The behavior of the BEGINROUTES statement is the same as the GATEWAY statement but allows a BSD style syntax to be specified for destination IP address and address mask and IPv6 address and prefix.	Changed in z/OS CS V1R4
BEGINVTAM / ENDVTAM	TELNET statement — see “BEGINVTAM information block” on page 206 for details.	
DELETE DEVICE	The DELETE DEVICE statement is used to delete a previously defined device. In z/OS CS V1R4, it is supported for virtual devices.	Changed in z/OS CS V1R4
DELETE LINK	The DELETE LINK statement is used to delete a previously defined link. In z/OS CS V1R4, it is supported for virtual links.	Changed in z/OS CS V1R4

Table 18. New or changed PROFILE.TCPIP configuration statements and parameters (continued)

Statement or parm	Description	Status
DELETE PORT	The DELETE PORT statement is used to unreserve a port for a specified jobname. In z/OS CS V1R4, the processing of BIND IP address is changed to allow either an IPv4 or fully qualified IPv6 address.	Changed in z/OS CS V1R4
DEVICE for CLAW devices	PACKED keyword: Enables packing of small packets into 4K frames.	New in CS for OS/390 V2R10
	Changed to allow for packing buffers up to 60K.	Changed in z/OS CS V1R2
DEVICE and LINK for MPCIPA devices	Defines MPCIPA devices and links for OSA-Express with gigabit ethernet adapter. In V2R10, also for OSA-Express with Fast Ethernet or ATM LAN-emulation adapters. New link type, IPAQENET, is supported for MCPIPA devices. The same link type is used to define OSA-Express gigabit ethernet, fast ethernet, or ATM LAN-emulation adapters.	Changed in CS for OS/390 V2R10
	IPAQTR added to indicate that the link uses the IP Assist based interface, belongs to the QDIO family of interfaces, and uses the Token Ring protocol. IPAQIDIO added. It is used to manually configure a HiperSockets device and link.	Changed in z/OS CS V1R2
GLOBALCONFIG	Statement to define global values for TCP/IP stack. Changed in z/OS CS V1R2 to define the values being used for ECSALIMIT and POOLLIMIT.	Changed in z/OS CS V1R2
HOME	Statement to provide the list of home addresses and associated link names. Note that in V2R6 and later, IP addresses in the range 127.0.0.128 thru 127.0.0.255 are reserved for IBM use and cannot be coded on the HOME statement as the IP address of any interface, including LOOPBACK.	Changed in z/OS CS V1R2
INTERFACE	Statement that is used to configure an IPv6 interface.	New in z/OS CS V1R4
INTERNAL - CLIENTPARMS	TELNET statement — see “TELNETPARMS information block” on page 205 for details.	
IPCONFIG	The IPCONFIG statement is used to update the IP layer of TCP/IP. Enhanced to define the iQDIO routing capability with the IQDIOROUTING QDIOPRIORITY parameter.	Changed in z/OS CS V1R2
	Enhanced with the TCPSTACKSOURCEVIPA option. This allows you to specify source Dynamic VIPA for outbound TCP connections.	Changed in z/OS CS V1R4
	DVIPSEC subparameter of the FIREWALL parameter added to enable Sysplex Wide Security Association. FORMAT keyword added. It only applies to stacks that are not enabled for IPv6.	
IPCONFIG6	Statement to update the IP layer of TCP/IP with information that pertains to IPv6.	New in z/OS CS V1R4
LINK	See DEVICE and LINK statement descriptions in this table.	

Table 18. New or changed PROFILE.TCPIP configuration statements and parameters (continued)

Statement or parm	Description	Status
NETACCESS / ENDNETACCESS	Statement to configure which SAF resource names are used to control outbound requests to particular networks or hosts.	New in CS for OS/390 V2R10
	In z/OS CS V1R4, updated to add new parameters (INBound/NOINBound and OUTBound/NOOUTBound) to activate netaccess inbound and outbound support.	Changed in z/OS CS V1R4
PKTTRACE	The PKTTRACE statement and VARY TCPIP,,PKTTRACE command are used to control the packet tracing facility in TCP/IP.	Changed in z/OS CS V1R4
	The processing of IP= parameter is changed in z/OS CS V1R4 to allow either an IPv4 or IPv6 address. The IP parameter also supports the use of CIDR notation for an IPv4 address mask or IPv6 prefix length.	
	The INTFNAME parameter is used to specify the name of an IPv6 network interface.	New in z/OS CS V1R4
PORT	The PORT statement is used to reserve a port for a specified jobname. In V2R10, the following changes were made: <ul style="list-style-type: none"> • A BIND IP address option was added. It may be used for applications that bind to INADDR_ANY to convert the BIND request to one that binds to a specific IP address. • User may now be specified as RESERVED to prevent use of a particular port or * to allow it to be used by any user. • A SAF keyword was added to allow the definition of a SAF resource name that defines the SAF resource definition that controls which users may bind to the port. 	Changed in CS for OS/390 V2R10
	In z/OS CS V1R2, the OPTMSS option is retired, as it no longer provides a performance benefit.	Changed in z/OS CS V1R2
	In z/OS CS V1R4, the processing of BIND IP address changed to allow either an IPv4 or fully qualified IPv6 address.	Changed in z/OS CS V1R4
PORTRANGE	In V2R10: <ul style="list-style-type: none"> • User may now be specified as RESERVED to prevent use of a particular portrange or * to allow it to be used by any user. • New SAF keyword to allow definition of SAF resource name that defines the SAF resource definition that controls which users may bind to the portrange. 	Changed in V2R10 and in z/OS CS V1R2
	In z/OS CS V1R2, the OPTMSS option is retired, as it no longer provides a performance benefit.	
ROUTE	Statement in BEGINROUTES block to define static routes to the IP route table using a BSD style syntax for destination IP address and address mask.	New in CS for OS/390 V2R10
	REPLACEABLE option for static routes added.	Changed in z/OS CS V1R2
	The destination IP address changed to support either an IPv4 address or an IPv6 address (either fully qualified or in IP address/prefix len format.) The first hop gateway IP address is also changed to support either IPv4 or fully qualified IPv6 addresses.	Changed in z/OS CS V1R4

Table 18. New or changed PROFILE.TCPIP configuration statements and parameters (continued)

Statement or parm	Description	Status
SACONFIG	<p>Specifies parameters for the TCP/IP SNMP subagent.</p> <p>In V2R10, ATMENABLED replaced by the new OSAENABLED parameter. OSADISABLED is a new parameter to allow SNMP subagent support for OSA-related MIB objects to be turned off.</p> <p>Also in V2R10, the values of the COMMUNITY and AGENT parameters are no longer set to their default values of public and 161, respectively, when processing a V TCPIP,,OBEYFILE for the SACONFIG Profile statement.</p>	Changed in CS for OS/390 V2R10
SMFCONFIG	Statement changed to define the SMF configured settings under two new subsections: one for SMF record type 118 and one for type 119.	Changed in z/OS CS V1R2
TCPCONFIG	<p>Specifies TCP parameters.</p> <p>Parameters added for FINWAIT2TIME (the number of seconds a TCP connection should remain in the FINWAIT2 state) and TCPTIMESTAMP (TCP Timestamp Option).</p>	Changed in z/OS CS V1R2
TELNETPARMS	TELNET statement — see “TELNETPARMS information block” on page 205 for details.	
VIPABACKUP	Statement in VIPADYNAMIC block to designate Dynamic VIPAs for which this stack will provide automatic backup when the owning stack fails.	New in CS for OS/390 V2R8
VIPADEFINE	<p>Statement in VIPADYNAMIC block to designate Dynamic VIPAs which this stack should initially own and support.</p> <p>In V2R10, MOVEABLE is parameter to provide immediate non-disruptive (or disruptive) movement of dynamic VIPAs from one stack to another.</p> <p>In z/OS CS V1R2, a keyword, SERVICEMGR, indicates that Sysplex Distributor will perform the Cisco MNLB Service Manager Function for distributed dynamic VIPAs. This keyword is optional and has no effect if there is no VIPADISTRIBUTE DEFINE statement for this VIPA.</p>	Changed in CS for OS/390 V2R10 and z/OS CS V1R2
VIPADISTRIBUTE	<p>Statement to define or delete a definition for a dynamic VIPA for which new connection requests may be distributed to other TCP/IP stacks in the sysplex.</p> <p>In z/OS CS V1R4, the SYSPLEXEXPORTS option is added. This is used when the corresponding application has been configured with VIPADSOURCE for the same IP address as is specified on the VIPADISTRIBUTE statement.</p>	New in CS for OS/390 V2R10, changed in z/OS CS V1R4
VIPARANGE	In V2R10, MOVEABLE is new parameter to provide immediate non-disruptive (or disruptive) movement of a dynamic VIPAs from one stack to another.	Changed in CS for OS/390 V2R10
VIPASMPARMS	Provides the parameters needed by Sysplex Distributor to perform the Cisco MNLB Service Manager Function for distributed dynamic VIPAs	New in z/OS CS V1R2

SYS1.PARMLIB members

Table 19. New or changed SYS1.PARMLIB members

Member	Entry	Description	Status
BPXPRMxx	FILESYSTYPE	Information about Physical File Systems. NETWORK definition for AF_INET6 domain now supported.	New in CS for OS/390 V2R10
	RESOLVER_PROC	Specifies the procedure name, if any, to be used to start the resolver address space.	New in z/OS CS V1R2
CTIEZB00	OPTIONS	Component trace options for SYSTCPIP component.	
		Added options ACCESS, ROUTE, and SOCKAPI. Groups also added. Two options deleted: SYSCALL and CTC. In addition, the maximum trace buffer size is increased to 256M.	Changed in CS for OS/390 V2R10
		Added option POLICY to option list.	Added in z/OS CS V1R2
		Removed option SOCKAPI from the group option ALL. IPv6 addresses and prefixes (1-128) can be specified for the IPADDR filter keyword. A numeric IPv4 address prefix (1-32) can be specified after an IPv4 address filter. Added new trace option ND (Neighbor Discovery) which is an alias for the ARP trace option.	Changed in z/OS CS V1R4
CTIIDS00		Added parmlib member for Intrusion Detection Services.	New in z/OS CS V1R2
CTIRES00		Added parmlib member for specifying CTRACE settings for the resolver.	New in z/OS CS V1R2
EZAIPCSP		IPCS exit definitions	New in CS for OS/390 V2R10
IKJTSOxx		TSO uses IKJTSOxx to determine which commands and programs are authorized. In V2R10, the TSO commands LPQ, LPRM, LPR, and RSH can now be authorized. Commands to be run in authorized state must be listed in IKJTSOxx using the AUTHCMDS NAMES statement.	Changed in CS for OS/390 V2R10
		Changed to add PING under AUTHCMD NAMES.	Changed in z/OS CS V1R4
PROGxx	APF	The name of the load library SEZALINK was changed to SEZALOAD. You must update PROGxx to APF authorize SYS1.SEZALOAD.	Changed in z/OS CS V1R4

Operator commands

Table 20. New or changed operator commands

Command	Parameters	Description	Status
DISPLAY TCPIP,,HELP		Displays syntax of TCP/IP operator commands; updated each release to display help information for new DISPLAY TCPIP command parameters.	
	ACCess	Displays help on NETSTAT ACCess command.	New in CS for OS/390 V2R10
	IDS	Displays information about intrusion detection services.	New in z/OS CS V1R2
	ND	Displays help on NETSTAT ND command.	New in z/OS CS V1R4
	PURGECACHE	Displays help on the PURGECACHE command.	New in z/OS CS V1R4
	STATS	Displays help on NETSTAT STATS command.	New in z/OS CS V1R2
	STOR	Displays help on STOR command.	New in CS for OS/390 V2R10
	VCRT	Displays help on NETSTAT VCRT command.	New in CS for OS/390 V2R10
	VDPT	Displays help on NETSTAT VDPT command.	New in CS for OS/390 V2R10
	VIPADCFG	Displays help on NETSTAT VIPADCFG command.	New in CS for OS/390 V2R10
DISPLAY TCPIP,,NETSTAT		Requests NETSTAT information. Starting in z/OS CS V1R4, the following Netstat reports support IPv6 information: <ul style="list-style-type: none"> • ALLCONN • BYTEINFO • CONFIG • CONN • DEVLINKS • HOME • PORTLIST • ROUTE • SOCKETS • STATS 	
	ACCess, NETWork	Option to display the TCP/IP profile network access definitions.	New in CS for OS/390 V2R10
	ALLConn	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
	ARp	The ARP report now contains ARP data for some devices that provide an ARP offload function. Refer to "Devices Which Support ARP Offload" in <i>z/OS Communications Server: IP Configuration Guide</i> .	Changed in CS for OS/390 V2R10
		Changed so that no MAC address or MAC address type is displayed for iQDIO (HiperSockets) links.	Changed in z/OS CS V1R2
	BYTEinfo	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
The bytes in and out fields are enhanced to support 64-bit counters when the long format display is requested.		Changed in z/OS CS V1R4	

Table 20. New or changed operator commands (continued)

Command	Parameters	Description	Status
DISPLAY TCPIP,,NETSTAT continued	CONFIG	Changed to move dynamic VIPA configuration information to VIPADCFG.	Changed in CS for OS/390 V2R10
		Report changed as follows: <ul style="list-style-type: none"> Information is displayed about the FinWait2Time and TcpTimeStamp defined in the TCPCONFIG profile statement. The SMF configured settings are displayed under two new subsections: one for SMF record type 118 and one for type 119. Report enhanced to replace existing TcpFlags field and UdpFlags field with their byte definitions. The TCP/IP storage usage information or the service level of a TCP/IP module is displayed (it will show the values being used for ECSALIMIT and POOLLIMIT). 	Changed in z/OS CS V1R2
		Report enhanced to display the following: <ul style="list-style-type: none"> Sysplex-wide Dynamic Source VIPAs for TCP connections information. The setting of the new DVIPSEC/NODVIPSEC subparameter from the IPCONFIG profile statement. The IP configuration setting with value of Yes or No instead of value of 00001 or 00000. The FORMAT information defined in the IPCONFIG profile statement. The IPv6 configuration table (displayed only when the stack is IPv6 enabled). If the IpAddr/PrefixLen format was used to define the data trace, then the IpAddr/PrefixLen field name will be displayed in the Data Trace Setting instead of IpAddr and SubNet field names. 	Changed in z/OS CS V1R4
	COnn	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2

Table 20. New or changed operator commands (continued)

Command	Parameters	Description	Status
DISPLAY TCPIP,,NETSTAT continued	DEvlinks	Display has been enhanced to indicate: <ul style="list-style-type: none"> • Which devices perform an ARP offload function and to indicate whether the ARP cache data and ARP counters can be retrieved from the device by the TCP/IP stack. • The configured and actual router status and adapter link speed for MPCIPA devices. • The device status in addition to link status. The field name for link status is changed from STATUS to LNKSTATUS. As of V2R10, OSA-Express Gigabit Ethernet, Fast Ethernet, and ATM LAN-emulation adapters will all be displayed as link type IPAQENET.	Changed in CS for OS/390 V2R10
		Report enhanced to display: <ul style="list-style-type: none"> • Information for the iQDIO (HiperSockets) device. • The configured and actual packing modes for CLAW devices. The new CfgPacking field contains the configured packing mode, and the new ActPacking field contains the actual Packing mode. If the DEVICE is not yet started, then the value for Actpacking field will be Unknown. • 64-bit BytesIn and BytesOut counters for an interface. 	Changed in z/OS CS V1R2

Table 20. New or changed operator commands (continued)

Command	Parameters	Description	Status
DISPLAY TCPIP,,NETSTAT continued	DEvlinks continued	Report display is changed in the following ways: <ul style="list-style-type: none"> IPv6 interface types LOOPBACK6, VIRTUAL6, and IPAQENET6 are displayed. The ARP offload and BSDROUTINGPARMS information are not supported and are therefore not displayed for IPv6 interfaces. The CfgRouter and ActRouter fields are moved from the device portion of the display to the link portion for IPv6 interfaces. This is also true for IPv4 when the LONG format is in effect. For IPv6 interfaces, the display uses field names IntfName, IntfType, and IntfStatus whereas for IPv4 links the display uses field names LnkName, LnkType, and LnkStatus respectively. The SOURCEVIPAINTERFACE information is added for IPv6 interfaces. The field name ArpMacAddress is changed to MacAddrOrder for IPv4 links. The field name BroadcastCapability is changed to IpBroadcastCapability for IPv4 TR links. The field name BroadcastType is changed to ArpBroadcastType for IPv4 TR links. For IPv6 interfaces, the Packet Trace Setting display uses field name IpAddr/PrefixLen. For IPv4 links, if IpAddr/PrefixLen format was used to define the packet trace, then the IpAddr/PrefixLen field name will be used instead of IpAddr and SubNet field names. A new RtrHopLimit field is added for IPv6 interfaces. The DevNum field will no longer be shown for device types other than CTC, CLAW, LCS, CDLC. The MAC address for links on LCS devices and IPAQENET6 interfaces is displayed. The INTFName filter is added to provide the response on the specified link or interface name. Both configured and actual MTU information is added for IPAQENET6 interfaces. The actual MTU information is added for non-VIPA IPv4 links and IPv6 interfaces. A new interface state is added for Duplicate Address Detection (DAD) that is in progress for the link local address on the IPV6 interface. For IPv6 interfaces, display the multicast group IP address as the last object on the line. 	Changed in z/OS CS V1R4
DISPLAY TCPIP,,NETSTAT continued	FORMat	Controls the Netstat report in a given format.	New in z/OS CS V1R4
	Home	Displays home addresses. In z/OS CS V1R4, the following changes are made: <ul style="list-style-type: none"> The address type and new flag values are added for IPv6 support. The list of unavailable IPv6 home addresses is displayed when the stack is IPv6 enabled. 	Changed in z/OS CS V1R4
	IDS	Displays information about intrusion detection services.	New in z/OS CS V1R2

Table 20. New or changed operator commands (continued)

Command	Parameters	Description	Status
DISPLAY TCPIP,,NETSTAT continued	ND	Displays neighbor discovery information.	New in z/OS CS V1R4
	PORTLIST	The OPTMSS parameter is no longer supported from the TCP/IP profile statements; therefore, the 'O' flag is removed from the report.	Changed in z/OS CS V1R4
	ROUTE	Display will show additional routes that were not shown in previous releases. All implicit routes from LOOPBACK and HOME statements will be shown, and a new route type for PathMTU Hosts will be displayed.	Changed in CS for OS/390 V2R10
		Keywords added: <ul style="list-style-type: none"> IQDIO is added to display the entries in the iQDIO (HiperSockets) routing table. RSTAT is added to display all of the static routes that are defined as replaceable. 	Changed in z/OS CS V1R2
		The following changes were made in z/OS CS V1R4: <ul style="list-style-type: none"> The DETAIL keyword is added to display more detailed information per routing entry. Two routing tables, one for IPv4 destinations and one for IPv6 destinations, are displayed in the report. The ADDRATYPE keyword is added with a choice of IPV4 or IPV6 to include only IPv4 or IPv6 in the report. When filtering a response on a specified IP address, the DEFAULT and DEFAULTNET routes are no longer returned. 	Changed in z/OS CS V1R4
	SOCKets	The following changes were made: <ul style="list-style-type: none"> The NOTN3270 filter is added to exclude TN3270 server connections from the report. The existing filter support is enhanced so that the report can provide the response on the specified client name, IP address, or port number. 	Changed in z/OS CS V1R2
	STATS	Displays performance statistics.	New in z/OS CS V1R2
The IPv6 and ICMPv6 statistics are displayed when the stack is IPv6 enabled.		Changed in z/OS CS V1R4	

Table 20. New or changed operator commands (continued)

Command	Parameters	Description	Status
DISPLAY TCPIP,,NETSTAT continued	VCRT	Option to display the dynamic VIPA Connection Routing Table information.	New in CS for OS/390 V2R10
		Keyword DETAIL is added to display the the policy rule and action names for each dynamic VIPA connection.	Changed in z/OS CS V1R2
	VDPT	Option to display the dynamic VIPA Destination Port Table information.	New in CS for OS/390 V2R10
		Changed to add the QoS Policy Action name.	Changed in z/OS CS V1R2
	VIPADCFG	Option to display dynamic VIPA configuration information.	New in CS for OS/390 V2R10
Enhanced to display Sysplexports information.		Changed in z/OS CS V1R4	
VIPADyn	Display is enhanced to indicate whether the stack is both the distributing stack and a new connection destination stack for this Dynamic VIPA IP Address.	Changed in CS for OS/390 V2R10	
DISPLAY TCPIP,,STOR	MODULE	New option to display module prefix information (compile date, and so on) for most TCP/IP stack, PFS layer, and Telnet modules.	New in CS for OS/390 V2R10
	STOR	Displays general TCP/IP storage information.	Changed in z/OS CS V1R2
DISPLAY TCPIP,,SYSPLEX	VIPADYN	Display is enhanced to show dynamic VIPAs for a stack which are able to receive incoming connection requests, but which are not advertised to that stack's attached routing daemon.	Changed in CS for OS/390 V2R10
DISPLAY TCPIP,, TELNET		See "Telnet operator commands" on page 209.	
MODIFY PAGENT_procname	Parameters include: LOGLEVEL, DEBUG, TRACE, QUERY, and REFRESH	Allows policies to be refreshed immediately, and also allows the log, debug, and trace levels to be changed dynamically.	New in z/OS V1R2
MODIFY RESOLVER_ procname	DISPLAY	Displays the current names of the GlobalTCPIPData and DefaultTCPIPData values.	New in z/OS CS V1R2
		In V1R4, also displays the current names of GlobalIPNODES, DefaultIPNODES and the value of COMMONSEARCH/NOCOMMONSEARCH.	Changed in z/OS CS V1R4
	REFRESH and REFRESH, SETUP=	Allows you to change the values of the TCPIP.DATA statements in the GlobalTCPIPData and DefaultTCPIPData.	New in z/OS CS V1R2
		In V1R4, also allows you to change GlobalIPNODES and DefaultIPNODES files, or just the contents in the current GlobalIPNODES and DefaultIPNODES files, and the value of COMMONSEARCH/NOCOMMONSEARCH.	Changed in z/OS CS V1R4
MODIFY remote_execution _server_procname	PURGE	Allows control over whether or not the job output is purged upon completion of the job.	New in CS for OS/390 V2R10

Table 20. New or changed operator commands (continued)

Command	Parameters	Description	Status
TRACE CT,ON,COMP= SYSTCPIP	OPTIONS	Turns on component trace for TCP/IP address space.	Changed in CS for OS/390 V2R10
		V2R10 introduces the following enhancements: <ul style="list-style-type: none"> • New CTRACE options: SOCKAPI, ROUTE, and ACCESS. • CTRACE options CTC and SYSCALL are deleted. • Some CTRACE options are combined so that if you turn on one, you get all. If you turn off one, they all turn off. <ul style="list-style-type: none"> – OPCMDS, OPMSGs, and INIT are combined. – ENGINE and QUEUE are combined. • CTRACE option groups are created to turn on multiple options concurrently to facilitate trace collection based on the type of problem being seen. 	
		POLICY option list - Turns on the POLICY option to trace usage of Policy based rules and actions.	New in z/OS CS V1R2
TRACE CT,ON,COMP= SYSTCPIS		Turns on the component trace for the Traffic Regulation and Intrusion Detection. By default, this is on.	New in z/OS CS V1R2
TRACE CT,ON,COMP= SYSTCPRE,SUB= (resolverprocname)		Turns on the component trace for the resolver.	New in z/OS CS V1R2
VARY TCPIP,,DATTRACE		The VARY TCPIP,,DATTRACE command is used to trace socket data (transforms) into and out of the physical file structure (PFS).	Changed in z/OS CS V1R4
	IP	The processing of IP= parameter is changed in z/OS CS V1R4 to allow either an IPv4 or IPv6 address. The IP parameter is also changed to support the use of CIDR notation for an IPv4 address mask or IPv6 prefix length.	Changed in z/OS CS V1R4
	INTFNAME	Specifies the name of an IPv6 network interface.	New in z/OS CS V1R4
VARY TCPIP,,PKTTRACE		The PKTTRACE statement and VARY TCPIP,,PKTTRACE command are used to control the packet tracing facility in TCP/IP.	Changed in z/OS CS V1R4
	IP	The processing of IP= parameter is changed in z/OS CS V1R4 to allow either an IPv4 or IPv6 address. The IP parameter is also changed to support the use of CIDR notation for an IPv4 address mask or IPv6 prefix length.	Changed in z/OS CS V1R4
	INTFNAME	Specifies the name of an IPv6 network interface.	New in z/OS CS V1R4
VARY TCPIP,,PURGECache		This command will purge the ARP or Neighbor cache for the requested Link or Interface. If an IPv4 link name is specified, the ARP cache for the requested link is purged. If an IPv6 interface name is specified, the Neighbor cache for the requested interface is purged.	New in z/OS CS V1R4
VARY TCPIP,,TELNET		See Table 140 on page 209.	

TSO commands

Table 21. New or changed TSO commands

Command	Parameter	Description	Status
DIG		<p>Queries a name server.</p> <p>A DIG command -envsav option from a release prior to z/OS CS V1R2 is not compatible with z/OS CS V1R2; a message will be issued and the defaults will be used.</p> <p>Prior to z/OS CS V1R2, the stats option for the DIG command included <i>round trip time</i>. In z/OS CS V1R2, <i>round trip time</i> is <i>not</i> included as a statistic.</p>	Changed in z/OS CS V1R2
HOMETEST		In z/OS CS V1R2, the message "EZA0620I The TCP/IP system parameter file used will be..." is no longer issued. Use the Trace Resolver output to determine which TCPIP.DATA statements are being used. Refer to <i>z/OS Communications Server: IP Configuration Guide</i> for more information about using HOMETEST.	Changed in z/OS CS V1R2
NETSTAT		<p>Displays the network status of the local host. Starting in z/OS CS V1R4, the following Netstat reports support IPv6 information:</p> <ul style="list-style-type: none"> • ALL • ALLCONN • BYTEINFO • CONFIG • CONN • DEVLINKS • HOME • PORTLIST • ROUTE • SOCKETS • STATS • TELNET • UP 	
	ALL	In V2R10, the display now includes policy rule.	Changed in CS for OS/390 V2R10
		<p>The following enhancements were made:</p> <ul style="list-style-type: none"> • The NOTN3270 filter is added to exclude TN3270 server connections from the report. • The report is enhanced to display TCP server backlog and accept counters for every server connection, and to display TCP send buffer size for all TCP connections. • The report provides the response on the specified IP address, or port number. 	Changed in z/OS CS V1R2
		<p>The following enhancements were made:</p> <ul style="list-style-type: none"> • The bytes in and out fields, segments in and out fields, and datagram in and out fields are enhanced to support 64-bit counters when the long format display is requested. • The OPTMSS parameter is no longer supported from the TCP/IP profile statements; therefore, the OptMaxSegmentSize field was removed from the report. 	Changed in z/OS CS V1R4
	ALLConn	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2

Table 21. New or changed TSO commands (continued)

Command	Parameter	Description	Status
NETSTAT continued	ARp	The ARP report now contains ARP data for some devices that provide an ARP offload function. Refer to "Devices Which Support ARP Offload" in <i>z/OS Communications Server: IP Configuration Guide</i> .	Changed in CS for OS/390 V2R10
		Changed so that no MAC address or MAC address type is displayed for iQDIO (HiperSockets) links.	Changed in z/OS CS V1R2
	BYTEinfo	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
		The bytes in and out fields are enhanced to support 64-bit counters when the long format display is requested.	Changed in z/OS CS V1R4
	CLients	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
	COnn	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
NETSTAT continued	CONFIG	Report changed to move dynamic VIPA configuration information into a new VIPADCFG.	Changed in CS for OS/390 V2R10
		Report updated and enhanced to display the following: <ul style="list-style-type: none"> The SMF configured settings under two new subsections: one for SMF record type 118 and one for type 119. Information about the FinWait2Time and TcpTimeStamp defined in TCPCONFIG profile statement. The byte definitions of the TcpFlags and UdpFlags fields (the byte definitions replaced the existing field values) The TCP/IP storage usage information or the service level of a TCP/IP module (it will show the values being used for ECSALIMIT and POOLLIMIT). 	Changed in z/OS CS V1R2
		Report enhanced to display the following: <ul style="list-style-type: none"> Sysplex-wide Dynamic Source VIPAs for TCP connections information. The setting of the new DVIPSEC/NODVIPSEC subparameter from the IPCONFIG profile statement. The IP configuration setting with value of Yes or No instead of value of 00001 or 00000. The FORMAT information defined in the IPCONFIG profile statement. The IPv6 configuration table (displayed only when the stack is IPv6 enabled). If the IpAddr/PrefixLen format was used to define the data trace, then the IpAddr/PrefixLen field name will be displayed in the Data Trace Setting instead of IpAddr and SubNet field names. 	Changed in z/OS CS V1R4

Table 21. New or changed TSO commands (continued)

Command	Parameter	Description	Status
NETSTAT continued	DEVlinks	<p>Display has been enhanced to indicate:</p> <ul style="list-style-type: none"> • Which devices perform an ARP offload function and to indicate whether the ARP cache data and ARP counters can be retrieved from the device by the TCP/IP stack. • The configured and actual router status and adapter link speed for MPCIPA devices. • The device status in addition to link status. The field name for link status is changed from STATUS to LNKSTATUS. <p>As of V2R10, OSA-Express gigabit ethernet, fast ethernet, and ATM LAN-emulation adapters will all be displayed as link type IPAQENET.</p>	<p>Changed in CS for OS/390 V2R10</p>
		<p>Report enhanced to display the following:</p> <ul style="list-style-type: none"> • Information for the iQDIO (HiperSockets) device. • The configured and actual packing modes for CLAW devices. The new CfgPacking field contains the configured packing mode and the new ActPacking field contains the actual Packing mode. If the DEVICE is not yet started, then the value for Actpacking field will be Unknown. • 64-bit BytesIn and BytesOut counters for an interface. 	<p>Changed in z/OS CS for V1R2</p>

Table 21. New or changed TSO commands (continued)

Command	Parameter	Description	Status
NETSTAT continued	DEvlinks continued	<p>Report display is changed in the following ways:</p> <ul style="list-style-type: none"> • IPv6 interface types LOOPBACK6, VIRTUAL6, and IPAQENET6 are displayed. • The ARP offload and BSDROUTINGPARMS information are not supported and are therefore not displayed for IPv6 interfaces. • The CfgRouter and ActRouter fields are moved from the device portion of the display to the link portion for IPv6 interfaces. This is also true for IPv4 when the LONG format is in effect. • For IPv6 interfaces, the display uses field names IntfName, IntfType, and IntfStatus whereas for IPv4 links the display uses field names LnkName, LnkType, and LnkStatus respectively. • The SOURCEVIPAINTERFACE information is added for IPv6 interfaces. • The field name ArpMacAddress is changed to MacAddrOrder for IPv4 links. • The field name BroadcastCapability is changed to IpBroadcastCapability for IPv4 TR links. • The field name BroadcastType is changed to ArpBroadcastType for IPv4 TR links. • For IPv6 interfaces, the Packet Trace Setting display uses field name IpAddr/PrefixLen. For IPv4 links, if IpAddr/PrefixLen format was used to define the packet trace, then the IpAddr/PrefixLen field name will be used instead of IpAddr and SubNet field names. • A new RtrHopLimit field is added for IPv6 interfaces. • The DevNum field will no longer be shown for device types other than CTC, CLAW, LCS, CDLC. • The MAC address for links on LCS devices and IPAQENET6 interfaces is displayed. • The INTFName filter is added to provide the response on the specified link or interface name. • Both configured and actual MTU information is added for IPAQENET6 interfaces. The actual MTU information is added for non-VIPA IPv4 links and IPv6 interfaces. • A new interface state is added for Duplicate Address Detection (DAD) that is in progress for the link local address on the IPV6 interface. • For IPv6 interfaces, display the multicast group IP address as the last object on the line. 	Changed in z/OS CS V1R4
	FORMat	Controls the Netstat report in a given format.	New in z/OS CS for V1R4

Table 21. New or changed TSO commands (continued)

Command	Parameter	Description	Status
NETSTAT continued	GATE	Display will show additional routes that were not shown in previous releases. All implicit routes from LOOPBACK and HOME statements will be shown, and a new route type for PathMTU Hosts will be displayed.	Changed in CS for OS/390 V2R10
		When filtering a response on a specified IP address, the DEFAULT and DEFAULTNET routes are no longer returned.	Changed in z/OS CS for V1R4
	HELP	Changed to display the STATS.	Changed in z/OS CS V1R2
		Changed to display help on the -n option.	Changed in z/OS CS for V1R4
	Home	Displays home addresses. In z/OS CS V1R4, the following changes are made: <ul style="list-style-type: none"> The address type and new flag values are added for IPv6 support. The list of unavailable IPv6 home addresses is displayed when the stack is IPv6 enabled. 	Changed in z/OS CS V1R4
	IDS	Displays information about intrusion detection services.	New in z/OS CS V1R2
	ND	Displays neighbor discovery information.	New in z/OS CS V1R4
	PORTList	Changed to display the IP address and indicates whether a bind to INADDR_ANY will be converted to a BIND to the specified IP address.	Changed in CS for OS/390 V2R10
		The OPTMSS parameter is no longer supported from the TCP/IP profile statements, therefore, the 'O' flag is removed from the report.	Changed in z/OS CS V1R4
	ROUTE	Display will show additional routes that were not shown in previous releases. All implicit routes from LOOPBACK and HOME statements will be shown, and a new route type for PathMTU Hosts will be displayed.	Changed in CS for OS/390 V2R10
		Keywords added: <ul style="list-style-type: none"> Keyword IQDIO is added to display the entries in the iQDIO (HiperSockets) routing table. Keyword RSTAT is added to display all of the static routes that are defined as replaceable. 	Changed in z/OS CS V1R2
		The following changes were made in z/OS CS V1R4: <ul style="list-style-type: none"> The DETAIL keyword is added to display more detailed information per routing entry. Two routing tables, one for IPv4 destinations and one for IPv6 destinations, are displayed in the report. The ADDRTYPE keyword is added with a choice of IPV4 or IPV6 to include only IPv4 or IPv6 in the report. When filtering a response on a specified IP address, the DEFAULT and DEFAULTNET routes are no longer returned. 	Changed in z/OS CS V1R4

Table 21. New or changed TSO commands (continued)

Command	Parameter	Description	Status
NETSTAT continued	SLAP	Display changed to remove display of policy rules and policy actions. This information is now available by using the pasearch command. Also, a new field on the display will show the byte count of in-profile outbound data.	Changed in CS for OS/390 V2R10
		Display changed to remove display of Traffic Regulation (TR) policies. These policies are now part of Intrusion Detection Services (IDS) and can be displayed with Netstat IDS.	Changed in z/OS CS V1R2
	SOCKets	Enhancements include the following: <ul style="list-style-type: none"> Existing filter support enhanced so that the report can provide the response on the specified client name, IP address, or port number. The NOTN3270 filter is added to exclude TN3270 server connections from the report. 	Changed in z/OS CS V1R2
	STATS	Displays TCP/IP statistics for each protocol.	New in z/OS CS V1R2
		The IPv6 and ICMPv6 statistics are displayed when stack is IPv6 enabled.	Changed in z/OS CS V1R4
	TELnet	The bytes in and out fields are enhanced to support 64-bit counters when the long format display is requested.	Changed in z/OS CS V1R4
	Up	Displays the date and time that TCP/IP was started. In z/OS CS V1R4, display information is enhanced to also indicate whether or not the stack is IPv6 enabled.	Changed in z/OS CS V1R4
	VCRT	Option to display the dynamic VIPA Connection Routing Table information.	New in CS for OS/390 V2R10
		Keyword DETAIL is added to display the the policy rule and action names for each dynamic VIPA connection.	Changed in z/OS CS V1R2
	VDPT	Option to display the dynamic VIPA Destination Port Table information.	New in CS for OS/390 V2R10
		Changed to add the QoS Policy Action name.	Changed in z/OS CS V1R2
	VIPADCFG	Option to display dynamic VIPA configuration information.	New in CS for OS/390 V2R10
		Enhanced to display Sysplexports information.	Changed in z/OS CS V1R4
PING		The PING command sends an echo request to a node to determine whether the computer is accessible. In z/OS CS V1R4 it is rewritten to support IPv4 or IPv6 destinations.	Rewritten in z/OS CS V1R4
	host_name	Supports an IPv4 address, IPv6 address, or host name.	Changed z/OS CS V1R4
	ADDRTYPE	Specifies the IP address type that the Resolver should return when resolving the host name to an IP address.	New in z/OS CS V1R4
	INTF	Specifies the local interface over which the packets will be sent.	New in z/OS CS V1R4
	SRCIP	Specifies the source IP address to be used in the outbound packets.	New in z/OS CS V1R4
	TCP	Specifies the name of the TCP/IP stack through which PING tries to reach the target IP address.	New in z/OS CS V1R4

Table 21. New or changed TSO commands (continued)

Command	Parameter	Description	Status
TRACERTE		The TRACERTE command is useful for debugging various network problems. In z/OS CS V1R4 it is rewritten to support IPv4 or IPv6 destinations.	Rewritten in z/OS CS V1R4
	ADDRTYPE	Specifies the IP address type that the Resolver should return when resolving the host name to an IP address.	New in z/OS CS V1R4
	host_name	Supports an IPv4 address, IPv6 address, or host name.	Changed in z/OS CS V1R4
	INTF	Specifies the local interface over which the packets will be sent.	New in z/OS CS V1R4
	LIMDISP	Displays the received hop count.	New in z/OS CS V1R4
	NONAME	Bypasses received IP address to name resolution.	New in z/OS CS V1R4
	NOROUTE	Bypasses the normal routing tables.	New in z/OS CS V1R4
	PORT	Default port number changed to 33434.	Changed in z/OS CS V1R4
	SRCIP	Specifies the source IP address to be used in the outbound packets.	New in z/OS CS V1R4
	TCP	Specifies the name of the TCP/IP stack through which TRACERTE tries to reach the target IP address.	New in z/OS CS V1R4
	TOS	Specifies the Type of Service (ToS) value for an IPv4 destination.	New in z/OS CS V1R4
	VERBOSE	Displays additional messages.	New in z/OS CS V1R4

UNIX commands

Table 22. New or changed UNIX commands

Command	Parm	Description	Status
netstat		Synonym for onetstat in the z/OS UNIX System Services shell. See the onetstat entry in this table for updates.	

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
onetstat		Shows local network configuration and status of devices, gateways and connections. Starting in z/OS CS V1R4, the following onetstat reports support IPv6 addresses: -A, -a, -b, -c, -d, -f, -h, -o, -r, -s, -S, -t, and -u.	
	-?	Changed to display the new -S option.	Changed in z/OS CS V1R2
		Changed to display help on the ND option.	Changed in z/OS CS V1R4
	-A	In V2R10, the display now includes policy rule name.	Changed in CS for OS/390 V2R10
		The following enhancements were made: <ul style="list-style-type: none"> The NOTN3270 filter is added to exclude TN3270 server connections from the report. The report is enhanced to display TCP server backlog and accept counters for every server connection, and to display TCP send buffer size for all TCP connections. The report provides the response on the specified IP address, or port number. 	Changed in z/OS CS V1R2
		The following enhancements were made: <ul style="list-style-type: none"> The bytes in and out fields, segments in and out fields, and datagram in and out fields are enhanced to support 64-bit counters when the long format display is requested. The OPTMSS parameter is no longer supported from the TCP/IP profile statements; therefore, the OptMaxSegmentSize field was removed from the report. 	Changed in z/OS CS V1R4
	-a	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
	-b	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
The bytes in and out fields are enhanced to support 64-bit counters when the long format display is requested.		Changed in z/OS CS V1R4	

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
onetstat continued	-c	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
	-d	<p>Display has been enhanced to indicate:</p> <ul style="list-style-type: none"> • Which devices perform an ARP offload function and to indicate whether the ARP cache data and ARP counters can be retrieved from the device by the TCP/IP stack. • The configured and actual router status and adapter link speed for MPCIPA devices. • The device status in addition to link status. The field name for link status is changed from STATUS to LNKSTATUS. <p>As of V2R10, OSA-Express gigabit ethernet, fast ethernet, and ATM LAN-emulation adapters will all be displayed as link type IPAQENET.</p>	Changed in CS for OS/390 V2R10
		<p>Report enhanced to display the following:</p> <ul style="list-style-type: none"> • Information for the iQDIO (HiperSockets) device. • The configured and actual packing modes for CLAW devices. The new CfgPacking field contains the configured packing mode and the new ActPacking field contains the actual Packing mode. If the DEVICE is not yet started, then the value for Actpacking field will be Unknown. • 64-bit BytesIn and BytesOut counters for an interface. 	Changed in z/OS CS for V1R2

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
onetstat continued	-d continued	Report display is changed in the following ways: <ul style="list-style-type: none"> IPv6 interface types LOOPBACK6, VIRTUAL6, and IPAQENET6 are displayed. The ARP offload and BSDROUTINGPARMS information are not supported and are therefore not displayed for IPv6 interfaces. The CfgRouter and ActRouter fields are moved from the device portion of the display to the link portion for IPv6 interfaces. This is also true for IPv4 when the LONG format is in effect. For IPv6 interfaces, the display uses field names IntfName, IntfType, and IntfStatus whereas for IPv4 links the display uses field names LnkName, LnkType, and LnkStatus respectively. The SOURCEVIPINTERFACE information is added for IPv6 interfaces. The field name ArpMacAddress is changed to MacAddrOrder for IPv4 links. The field name BroadcastCapability is changed to IpBroadcastCapability for IPv4 TR links. The field name BroadcastType is changed to ArpBroadcastType for IPv4 TR links. For IPv6 interfaces, the Packet Trace Setting display uses field name IpAddr/PrefixLen. For IPv4 links, if IpAddr/PrefixLen format was used to define the packet trace, then the IpAddr/PrefixLen field name will be used instead of IpAddr and SubNet field names. A new RtrHopLimit field is added for IPv6 interfaces. The DevNum field will no longer be shown for device types other than CTC, CLAW, LCS, CDLC. The MAC address for links on LCS devices and IPAQENET6 interfaces is displayed. The INTFName filter is added to provide the response on the specified link or interface name. Both configured and actual MTU information is added for IPAQENET6 interfaces. The actual MTU information is added for non-VIPA IPv4 links and IPv6 interfaces. A new interface state is added for Duplicate Address Detection (DAD) that is in progress for the link local address on the IPV6 interface. For IPv6 interfaces, display the multicast group IP address as the last object on the line. 	Changed in z/OS CS for V1R4
	-e	The NOTN3270 filter is added to exclude TN3270 server connections from the report.	Changed in z/OS CS V1R2
	-F	Displays dynamic VIPA configuration information.	New in CS for OS/390 V2R10
		Displays Sysplexports information.	Changed in z/OS CS V1R4

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
onetstat continued	-f	Report changed to move dynamic VIPA configuration information into the new -F report.	Changed in CS for OS/390 V2R10
		Report updated and enhanced to display: <ul style="list-style-type: none"> The SMF configured settings under two new subsections: one for SMF record type 118 and one for type 119. Information about the FinWait2Time and TcpTimeStamp defined in TCPCONFIG profile statement. The byte definitions of the TcpFlags and UdpFlags fields (the byte definitions replaced the existing field values). The TCP/IP storage usage information or the service level of a TCP/IP module (it will show the values being used for ECSALIMIT and POOLLIMIT). 	Changed in z/OS CS V1R2
		Report enhanced to display the following: <ul style="list-style-type: none"> Sysplex-wide Dynamic Source VIPAs for TCP connections information. The setting of the new DVIPSEC/NODVIPSEC subparameter from the IPCONFIG profile statement. The IP configuration setting with value of Yes or No instead of value of 00001 or 00000. The FORMAT information defined in the IPCONFIG profile statement. The IPv6 configuration table (displayed only when the stack is IPv6 enabled). If the IpAddr/PrefixLen format was used to define the data trace, then the IpAddr/PrefixLen field name will be displayed in the Data Trace Setting instead of IpAddr and SubNet field names. 	Changed in z/OS CS V1R4
	-g	Display will show additional routes that were not shown in previous releases. All implicit routes from LOOPBACK and HOME statements will be shown, and a new route type for PathMTU Hosts will be displayed.	Changed in CS for OS/390 V2R10
		When filtering a response on a specified IP address, the DEFAULT and DEFAULTNET routes are no longer returned.	Changed in z/OS CS V1R4

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
onetstat continued	-h	Displays home addresses. In z/OS CS V1R4, the following changes are made: <ul style="list-style-type: none"> • The address type and new flag values are added for IPv6 support. • The list of unavailable IPv6 home addresses is displayed when the stack is IPv6 enabled. 	Changed in z/OS CS V1R4
	-j	Display changed to remove display of policy rules and policy actions. This information is now available by using the pasearch command. Also, a new field on the display will show the byte count of in-profile outbound data.	Changed in CS for OS/390 V2R10
		Display changed to remove display of Traffic Regulation (TR) policies. These policies are now part of Intrusion Detection Services (IDS) and can be displayed with onetstat -k.	Changed in z/OS CS V1R2
	-k	Displays information about intrusion detection services.	New in z/OS CS V1R2
	-M	Controls the Netstat report in a given format.	New in z/OS CS V1R4
	-n	Displays neighbor discovery information.	New in z/OS CS V1R4
	-O	Option to display the dynamic VIPA Destination Port Table information.	New in CS for OS/390 V2R10
		Changed to add the QoS Policy Action name.	Changed in z/OS CS V1R2
	-o	Report now displays the IP address and indicates whether a bind to INADDR_ANY will be converted to a bind to the specified IP address.	Changed in CS for OS/390 V2R10
		The OPTMSS parameter is no longer supported from the TCP/IP profile statements; therefore, the 'O' flag is removed from the report.	Changed in z/OS CS V1R4

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
onetstat continued	-R	The -R report now contains ARP data for some devices that provide an ARP offload function. Refer to "Devices Which Support ARP Offload" in <i>z/OS Communications Server: IP Configuration Guide</i> .	Changed in CS for OS/390 V2R10
		Changed so that no MAC address or MAC address type is displayed for iQDIO (HiperSockets) links.	Changed in z/OS CS V1R2
	-r	Display will show additional routes that were not shown in previous releases. All implicit routes from LOOPBACK and HOME statements will be shown, and a new route type for PathMTU Hosts will be displayed.	Changed in CS for OS/390 V2R10
		Keywords added: <ul style="list-style-type: none"> Keyword IQDIO is added to display the entries in the iQDIO (HiperSockets) routing table. Keyword RSTAT is added to display all of the static routes that are defined as replaceable. 	Changed in z/OS CS V1R2
		The following changes were made in z/OS CS V1R4: <ul style="list-style-type: none"> The DETAIL keyword is added to display more detailed information per routing entry. Two routing tables, one for IPv4 destinations and one for IPv6 destinations, are displayed in the report. The ADDRTYPE keyword is added with a choice of IPV4 or IPV6 to include only IPv4 or IPv6 in the report. When filtering a response on a specified IP address, the DEFAULT and DEFAULTNET routes are no longer returned. 	Changed in z/OS CS V1R4
	-S	Displays counters of performance characteristics to aid in identifying performance problems.	New in z/OS CS V1R2
		The IPv6 and ICMPv6 statistics are displayed when stack is IPv6 enabled.	Changed in z/OS CS V1R4
	-s	Enhancements include the following: <ul style="list-style-type: none"> Existing filter support enhanced so that the report can provide the response on the specified client name, IP address, or port number. The NOTN3270 filter is added to exclude TN3270 server connections from the report. 	Changed in z/OS CS V1R2
	-t	The bytes in and out fields are enhanced to support 64-bit counters when the long format display is requested.	Changed in z/OS CS V1R4
	-u	Displays the date and time that TCP/IP was started. In z/OS CS V1R4, display information is enhanced to also indicate whether or not the stack is IPv6 enabled.	Changed in z/OS CS V1R4
	-V	Option to display the dynamic VIPA Connection Routing Table information.	New in CS for OS/390 V2R10
		Keyword DETAIL is added to display the the policy rule and action names for each dynamic VIPA connection.	Changed in z/OS CS V1R2
-v	Display is enhanced to indicate whether the stack is both the distributing stack and a new connection destination stack for this Dynamic VIPA IP Address.	Changed in CS for OS/390 V2R10	

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
oping		Tests network connectivity of the local or remote host. In z/OS CS V1R4 it is rewritten to support IPv4 or IPv6 destinations.	
	host_name	Supports an IPv4 address, IPv6 address, or host name.	Changed in z/OS CS V1R4
	-A	Specifies the IP address type that the Resolver should return when resolving the host name to an IP address.	New in z/OS CS V1R4
	-i	Serves as a diagnostic aid in determining response times and path availability for Enhanced Multipath Load Balancing. In z/OS CS V1R4, it is changed to support either an IPv6 IP address or interface name.	Changed in z/OS CS V1R4
	-s	Specifies the source IP address to be used in the outbound packets.	New in z/OS CS V1R4
orouted		Starts OROUTED routing daemon.	
	-c	Assists with migration from OROUTED to OMPROUTE. With -c, OROUTED will create a file (using OROUTED configuration files) which can be used as the profile to start OMPROUTE.	New in z/OS CS V1R2
orshd	-k <i>mechanism</i>	Specifies the authentication mechanism to be used to authenticate the client. Valid values for mechanism are KRB5 and GSSAPI.	New in z/OS CS V1R2
	-e	Requires the client to encrypt the connection.	New in z/OS CS V1R2
	-m	Requires Kerberos 5 clients to present a cryptographic checksum of initial connection information, such as the name of the user that the client is trying to access in the initial authenticator.	New in z/OS CS V1R2
	-i	Ignores authenticator checksums if provided. This option ignores authenticator checksum presented by current Kerberos clients to protect initial connection information; it is the opposite of -m.	New in z/OS CS V1R2
otracert		Displays the route that a packet takes to reach the requested host. In z/OS CS V1R4, it is rewritten to trace route of packets to an IPv4 or IPv6 destination.	
	-A	Specifies the IP address type that the Resolver should return when resolving the host name to an IP address.	New in z/OS CS V1R4
	host_name	Supports an IPv4 address, IPv6 address, or host name.	Changed in z/OS CS V1R4
	-i	Specifies the local interface over which otracert packets will be sent. In z/OS CS V1R4, it is enhanced to support an IPv6 IP address or interface name.	New in CS for OS/390 V2R8; changed in z/OS CS V1R4
	-p	Default port number changed to 33434.	Changed in z/OS CS V1R4
	-s	Supports an IPv6 IP address.	Changed in z/OS CS V1R4

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
pagent	-l	Indicates the destination of the Policy Agent log file.	New in CS for OS/390 V2R10
	-d	Starting with V2R10, the -d parameter requires a numeric debug value. In previous releases, no parameter value was required.	Changed in CS for OS/390 V2R10
		New debug levels added.	Changed in z/OS CS V1R2
	-t or -T	Specifies whether to turn on LDAP client debugging.	New in z/OS CS V1R2
pasearch		Queries Policy Agent information.	New in CS for OS/390 V2R10
		Traffic Regulation (TR) policy is now part of Intrusion Detection Services (IDS). Output changed to display TR policy as IDS policy, not QOS policy. In addition, the authorization requirements are changed.	Changed in z/OS CS V1R2
ping		Synonym for oping in the z/OS UNIX System Services shell. See the oping entry in this table for updates.	
sntpd		A TCP/IP daemon that is used to provide the time in order to synchronize a network of (S)NTP clients. Simple network time protocol provides for a more accurate time than TIMED. SNTPD does not replace TIMED but it is the preferred server for synchronizing time in the network.	New in z/OS CS V1R4
	-d	Enables debugging. Activity logging and debug messages are written to stdout.	New in z/OS CS V1R4
	-df HFS-pathname	Enables debugging. Activity logging and debug messages are written to specified HFS file. Example: -df /var/sntpd.debug	New in z/OS CS V1R4
	-pf HFS-pathname	HFS path for pid file. Example: -pf /var	New in z/OS CS V1R4
	-m nnn	Acts in multicast mode. Sends multicast updates (TTL = 1) on all interfaces at every nnn seconds. Listens to multicast requests and responds with unicast replies.	New in z/OS CS V1R4
	-b nnn	Acts in broadcast mode. Sends local broadcasts on all interfaces every nnn seconds. Listens to broadcast requests and responds with unicast replies.	New in z/OS CS V1R4
	-?	Displays the syntax of the command usage/options.	New in z/OS CS V1R4
syslogd	-c	New invocation parameter to indicate that log files and directories should be created if they do not already exist.	New in CS for OS/390 V2R10
	-i	New invocation parameter to indicate that messages should not be received from the IP network.	New in CS for OS/390 V2R10
	-u	New invocation parameter to include user ID and job name in syslog records for records received over the AF_UNIX socket.	New in CS for OS/390 V2R10
traceroute		Synonym for otracert. See the otracert entry in this table for details.	Changed in z/OS CS V1R4

Table 22. New or changed UNIX commands (continued)

Command	Parm	Description	Status
trmd		Starts the Traffic Regulation Management Daemon. Collects and reports TRM logging and statistic data.	New in CS for OS/390 V2R10
		Expanded to support collection of logging and statistics data for Intrusion Detection Services (IDS), which includes TCP and UDP Traffic Regulation Management, Scan and Attack Detection.	Changed in z/OS CS V1R2
trmdstat		Extracts Traffic Regulation Management Daemon statistics from the syslog daemon output for analysis.	New in CS for OS/390 V2R10
		Supports additional reports for UDP Traffic Regulation, Attacks, and Scan Detection	Changed in z/OS CS V1R2

Environment variables

Table 23. Environment variables

Environment Variables	Appl	Description	Status
_BPXK_SETIBMOPT_TRANSPORT	Simple Network Time Protocol (SNTP)	Used to establish stack affinity for SNTPD.	New in z/OS V1R4
PAGENT_LOG_FILE_CONTROL	Policy Agent	Controls size and number of Policy Agent log files.	New in CS for OS/390 V2R10
OMPROUTE_DEBUG_FILE_CONTROL	OMPROUTE	Allows user to control size and number of trace files that OMPROUTE generates.	New in CS for OS/390 V2R10
RESOLVER_IPNODES	Resolver	Specifies which IPNODES file is used for the resolver name query.	New in z/OS CS V1R4
RESOLVER_TRACE	Resolver	Specifies where the resolver trace output will appear.	New in z/OS CS V1R2

Socket APIs

TCP/IP socket APIs enabled for IPv6 in z/OS CS V1R4

z/OS CS V1R4 introduces support for IPv6 addressing. Table 24 indicates which TCP/IP socket API commands are enabled for IPv6. **Y** indicates that yes, it is enabled for IPv6, and **N** indicates that No, it is not enabled for IPv6.

For details about enabling TCP/IP socket API commands for IPv6, refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* and *z/OS Communications Server: IP Application Programming Interface Guide*.

Table 24. Socket APIs enabled for IPv6

TCP/IP socket API command	Call Instruction API	Macro API	REXX API
ACCEPT	Y	Y	Y
BIND	Y	Y	Y
CONNECT	Y	Y	Y
FREEADDRINFO	Y	Y	N
GETADDRINFO	Y	Y	Y

Table 24. Socket APIs enabled for IPv6 (continued)

TCP/IP socket API command	Call Instruction API	Macro API	REXX API
GETCLIENTID	Y	Y	Y
GETNAMEINFO	Y	Y	Y
GETPEERNAME	Y	Y	Y
GETSOCKNAME	Y	Y	Y
GETSOCKOPT	Y	Y	Y
GIVESOCKET	Y	Y	Y
IOCTL	Y	Y	Y
NTOP	Y	Y	N
PTON	Y	Y	N
RECVFROM	Y	Y	Y
RECVMSG	Y	Y	N
SENDMSG	Y	Y	N
SENDTO	Y	Y	Y
SETSOCKOPT	Y	Y	Y
SOCKET	Y	Y	Y
TAKESOCKET	Y	Y	Y

Socket APIs

Table 25 includes the updates made to the socket APIs.

Refer to *z/OS C/C++ Run-Time Library Reference* for complete documentation of the z/OS UNIX C sockets APIs and refer to *z/OS UNIX System Services Programming: Assembler Callable Services Reference* for information about z/OS UNIX Assembler Callable Services. Refer to *z/OS Communications Server: IP Application Programming Interface Guide* for information about TCP/IP socket APIs.

Table 25. Socket APIs

Socket API	Command / Parameter	Description	Status
All socket APIs	Sendmsg() Sendto() BPX1SRX	These send commands allow a destination sockaddr to be specified. For a connected UDP or RAW socket, if a destination sockaddr is specified on the send command it must match the sockaddr specified in the earlier connect. The send command will be rejected with EISCONN if the sockaddrs do not match.	Changed in z/OS CS V1R4
C socket API	ioctl() / SIOCGIFFLAGS	IFF_VIRTUAL flag added to if.h flag, allowing SIOCGIFFLAGS to identify VIRTUAL interfaces (VIPAs).	Changed in CS for OS/390 V2R10

Table 25. Socket APIs (continued)

Socket API	Command / Parameter	Description	Status
C socket API	ioctl() / SIOCGMONDATA	ARP statistics are available for certain devices that support ARP offload. Refer to "Devices Which Support ARP Offload" in <i>z/OS Communications Server: IP Configuration Guide</i> .	Changed in CS for OS/390 V2R10
		Returns additional 64-bit interface counters and TCP/IP stack statistical counters.	Changed in z/OS CS V1R2
Call Instruction API and Macro API	GETSOCKOPT / SO_RCVBUF	Gets the size of the data portion of the TCP/IP receive buffer in OPTVAL.	Added parameter in V2R10
Call Instruction API and Macro API	IOCTL / SIOCGSPLXFQDN	Requests the fully qualified domain name for a given server and group name within a sysplex.	Added parameter in V2R10
Call Instruction API and Macro API	SETSOCKOPT / SO_RCVBUF	Sets the size of the data portion of the TCP/IP receive buffer in OPTVAL.	Added parameter in V2R10
Call Instruction API and Macro API	SETSOCKOPT / SO_SNDBUF	Sets the size of the data portion of the TCP/IP send buffer in OPTVAL.	Added parameter in V2R10
Macro API	GETHOSTBYNAME	Gets the IP address for the specified host name. NAME keyword is changed so that any trailing blanks are removed from the specified name prior to trying to resolve it to an IP address.	Changed in z/OS CS V1R2
Macro API	IOCTL / SIOCGMONDATA	ARP statistics are available for certain devices that support ARP offload. Refer to "Devices Which Support ARP Offload" in <i>z/OS Communications Server: IP Configuration Guide</i> .	Changed in CS for OS/390 V2R10
		Changed to return TCP/IP stack statistical counters.	Changed in z/OS CS V1R2
		Added IPv6 TCP/IP stack statistical counters.	Changed in z/OS CS V1R4
Call Instruction, Macro, C socket, and CICS socket APIs	GETSOCKOPT / TCP_NODELAY	Returns the status of Nagle algorithm (RFC 896).	New in z/OS CS V1R2
Call Instruction, Macro, C socket, and CICS socket APIs	SETSOCKOPT / TCP_NODELAY	Toggles the use of Nagle algorithm (RFC 896) for all data sent over the socket. This option is not supported for AF_IUCV sockets.	New in z/OS CS V1R2
Call Instruction, Macro, REXX, and CICS socket APIs	GETSOCKOPT / IP_MULTICAST_IF, IP_MULTICAST_LOOP and IP_MULTICAST_TTL	These new GETSOCKOPT commands allow the application to exploit IPv4 multicasting.	New in z/OS CS V1R4

Table 25. Socket APIs (continued)

Socket API	Command / Parameter	Description	Status
Call Instruction, Macro, REXX, and CICS socket APIs	SETSOCKOPT/ IP_ADD_MEMBERSHIP, IP_DROP_MEMBERSHIP, IP_MULTICAST_IF, IP_MULTICAST_LOOP and IP_MULTICAST_TTL	These new SETSOCKOPT commands allow the application to exploit IPv4 multicasting.	New in z/OS CS V1R4

IPCS subcommands

CTRACE COMP(SYSTCPDA) subcommand

The CTRACE COMP(SYSTCPDA) subcommand is the component name for packet data traces and it was new in z/OS CS V1R2.

Table 26. CTRACE COMP(SYSTCPDA) subcommand

Option	Description	Status
DEVTYPE	IPv6 types added: <ul style="list-style-type: none"> • LOOPBACK6 • VIRTUAL6 • IPAQENET6 	New in z/OS CS V1R4
FLAGS(FIC)	Supports IPv6.	Changed in z/OS CS V1R4
FLAGS(IPV4)	Select IPv4 packets.	New in z/OS CS V1R4
FLAGS(IPV6)	Select IPv6 packets.	New in z/OS CS V1R4
FLAGS(IPV6EXT)	Select packets that have an IPv6 extension header.	New in z/OS CS V1R4
FLAGS(LIC)	Supports IPv6.	Changed in z/OS CS V1R4
FLAGS(MIC)	Supports IPv6.	Changed in z/OS CS V1R4
FLAGS(OIC)	Supports IPv6.	Changed in z/OS CS V1R4
FLAGS(PING)	Select packets that are ICMP/ICMPv6 echo request and echo reply.	Changed in z/OS CS V1R4
ICMP6 or ICMPV6	Select packets with a protocol number of 58.	New in z/OS CS V1R4
INTERFACE	Select packet trace records with the specified INTERFACE name.	New in z/OS CS V1R4
IPADDR	Supports IPv6 addresses and the use of CIDR notation for an IPv4 address mask or IPv6 prefix length.	Changed in z/OS CS V1R4
IPADDR(L)	An IPv4 or IPv6 loopback address, 127.0.0.0/255.0.0.0 or ::1.	Changed in z/OS CS V1R4
IPADDR(O)	An IPv4 or IPv6 address of 0, 0.0.0.0/255.255.255.255 or ::/128.	Changed in z/OS CS V1R4
IPADDR(*)	Any address.	Changed in z/OS CS V1R4
IPV4	Equivalent to FLAGS(IPV4).	New in z/OS CS V1R4
IPV6	Equivalent to FLAGS(IPV6).	New in z/OS CS V1R4
LINKLOCAL	Select packets with an IPv6 link-local unicast address prefix. Equivalent to IPADDR(FE80::/10).	New in z/OS CS V1R4
LOOPBACK	An IPv4 or IPv6 loopback address, 127.0.0.0/255.0.0.0 or ::1.	Changed in z/OS CS V1R4
LOOPBACK6	Equivalent to IPADDR(::1).	New in z/OS CS V1R4

Table 26. CTRACE COMP(SYSTCPDA) subcommand (continued)

Option	Description	Status
MULTICAST	Select packets with an IPv4 or IPv6 multicast address. Equivalent to CLASSD IPADDR(FF00::/8).	New in z/OS CS V1R4
NTP	Equivalent to PORT(123).	New in z/OS CS V1R4
SITELOCAL	Select packets with an IPv6 site-local unicast address prefix. Equivalent to IPADDR(FEC0::/10).	New in z/OS CS V1R4
TRAFFICCLASS	Select the records with the matching IPv6 traffic class field.	New in z/OS CS V1R4

CTRACE COMP(SYSTCPIS) subcommand

The CTRACE COMP(SYSTCPIS) subcommand is the component name for Intrusion Detection Services packet traces and it was new in z/OS CS V1R2.

CTRACE COMP(SYSTCPRE) subcommand

The CTRACE COMP(SYSTCPRE) subcommand is the component name for resolver event traces and it was new in z/OS CS V1R2.

INETSTAT subcommand

The INETSTAT subcommand generates netstat information from a dump and it was removed in CS for OS/390 V2R10.

Table 27. INETSTAT subcommand

Option	Description	Status
-A	Provides detailed information about TCP/IP connections. Alternate command: TCPIP CS CONNECTION to get the connection ID, then TCPIP CS STREAM, TCPIP CS SOCKET, TCPIP CS TCB, OR TCPIP CS UDP (depending on the connection type) to display the detailed information	Removed in CS for OS/390 V2R10; use alternate command
-R	Queries the ARP cache information Alternate command: TCPIP CS TREE and TCPIP CS ROUTE	Removed in CS for OS/390 V2R10; use alternate command
-a	Shows summary information about all connections. Alternate command: TCPIP CS CONNECTION (ALL)	Removed in CS for OS/390 V2R10; use alternate command
-b	Displays the byte-count information about each connection. Alternate command: TCPIP CS TCB	Removed in CS for OS/390 V2R10; use alternate command
-c	Shows summary information about active connections. Alternate command: TCPIP CS CONNECTION	Removed in CS for OS/390 V2R10; use alternate command
-d	Displays information about devices and defined links in the TCP/IP address space. Alternate command: TCPIP CS CONFIG	Removed in CS for OS/390 V2R10; use alternate command
-e	Provides the client's authorization and the elapsed time since the client was last used. Alternate command: TCPIP CS TCB	Removed in CS for OS/390 V2R10; use alternate command
-g	Provides information about each gateway. Alternate command: TCPIP CS PROFILE	Removed in CS for OS/390 V2R10; use alternate command
-h	Displays the HOME list. Alternate command: TCPIP CS PROFILE	Removed in CS for OS/390 V2R10; use alternate command
-r	Displays routing information. Alternate command: TCPIP CS ROUTE	Removed in CS for OS/390 V2R10; use alternate command

Table 27. INETSTAT subcommand (continued)

Option	Description	Status
-s	Displays information about each client using the socket interface. Alternate command: TCIPPCS CONNECTION to get the connection ID, then TCIPPCS SOCKET to display the detailed information	Removed in CS for OS/390 V2R10; use alternate command
-u	Provides the date and time that TCP/IP was started. Alternate command: TCIPPCS STATE	Removed in CS for OS/390 V2R10; use alternate command

TCIPPCS subcommand

Table 28. TCIPPCS subcommand

Option	Description	Status
API	Displays information about the connects in the Sockets Extended Assembler Macro Application Programming Interface (Macro API) and the Pascal API.	Added in CS for OS/390 V2R10
CONNECTION	Displays summary information about all connections.	Added in CS for OS/390 V2R10
COUNTERS	Displays information about TCP/IP internal execution statistics.	New in z/OS CS V1R2
FIREWALL	Displays information about Firewall filters or tunnels.	Added in CS for OS/390 V2R10
FRCA	Displays information about the Fast Response Cache Accelerator (FRCA) connections or about cached objects.	Added in CS for OS/390 V2R10
HASH	Displays information about the structure of TCP/IP hash tables.	Added in CS for OS/390 V2R10
	The following changes were made in z/OS CS V1R4: <ul style="list-style-type: none"> • UDP added; it moved from TREE subcommand. • ICMPV6 added for HASH information for ICMPv6. 	Changed in z/OS CS V1R4
POLICY	Displays information about service policies.	Added in CS for OS/390 V2R10
RESOLVER	Displays information about the system resolver.	New in z/OS CS V1R2
ROUTE	iQDIO added for iQDIO route information	Changed in z/OS CS V1R4
	The following changes were made in z/OS CS V1R4: <ul style="list-style-type: none"> • ALL added for all route information in output. • IPV4 added for route information for IPv4 only. • IPV6 added for route information for IPv6 only. 	Changed in z/OS CS V1R4
SKSH	Displays the stream header control blocks. Removed in CS for OS/390 V2R10; use the TCIPPCS STREAM command instead.	Removed in CS for OS/390 V2R10
STREAMS	Displays the stream header control blocks. Replaces the SKSH command.	New in CS for OS/390 V2R10

Table 28. TCPIP CS subcommand (continued)

Option	Description	Status
TREE	iQDIO tree information added.	Changed in z/OS CS V1R2
	The following changes were made in z/OS CS V1R4: <ul style="list-style-type: none"> • UDP removed; it moved to HASH subcommand. • Neighbor Discovery tree information added. • ROUTEV4 added for route tree information for IPv4 only. • ROUTEV6 added for route tree information for IPv6 only. 	Changed in z/OS CS V1R4
VMCF	Displays information about VMCF (Virtual Machine Communication Facility) and IUCV (Inter-User Communication Vehicle) users.	Added in CS for OS/390 V2R10
XCF	Displays a cross-system coupling facility (XCF) analysis report.	Added in CS for OS/390 V2R10

Chapter 4. z/OS V1R4 Communications Server release summary

This chapter describes the major changes introduced in z/OS V1R4 Communications Server.

See Table 15 on page 23 for a complete list of the functional enhancements you should consider. See Chapter 3, “New and changed interfaces” on page 29 for information on new, changed, deleted, or obsolete statements, commands, and APIs.

For information about changes to File Transfer Protocol (FTP), see Chapter 9, “Migrating the FTP server and client” on page 167.

For information about changes to Telnet, see Chapter 10, “Migrating the Telnet server and client” on page 203.

For information about changes to Simple Network Management Protocol (SNMP), see Chapter 11, “Migrating the SNMP server and client” on page 231.

For information about changes to Domain Name Server (DNS), see Chapter 12, “Migrating to the BIND-based DNS name server” on page 249.

Migration considerations

This chapter consists of sections that describe the functions and enhancements new to z/OS V1R4 Communications Server, including any migration procedures. Consider the following as you migrate:

- This release introduces support for IPv6 addressing for certain functions and applications; see “IPv6 support” on page 79 for migration information that is pertinent if you choose to use the IPv6 support. Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for complete information on the IPv6 support of this release. It is a new publication and it introduces the design, concepts, and enablement considerations of using IPv6 support.
- All the IPv4 functions previously provided by z/OS CS are still supported in this release. You may choose to keep using IPv4 addressing for all your applications. The functional enhancements described in this document pertain only to IPv4 addressing unless specifically identified to be IPv6.
- The contents of the PDS SEZALINK load library were moved to the PDS/E SEZALOAD load library. Therefore, you must replace the name SEZALINK with the name SEZALOAD.
- The SEZAHHELP and AEZAHHELP data sets were replaced with HELP and AHELP, respectively; therefore, you must replace the name SEZAHHELP with the name HELP and you must replace the name AEZAHHELP with AHELP.
- The distribution library AEZAMOD1 was replaced with PDSE, AEZAMODS; therefore, you must replace the name AEZAMOD1 with AEZAMODS.
- The ASSORTEDPARMS and KEEPALIVEOPTIONS statements will not be supported in future releases. These two statements are no longer necessary and the use of ASSORTEDPARMS in combination with xxxCONFIG statements can produce undesired results. Therefore, IBM strongly recommends using:

- The GLOBALCONFIG, IPCONFIG, TCPCONFIG, and UDPCONFIG statements instead of the ASSORTEDPARMS statement. These other statements provide support for the parameters currently on the ASSORTEDPARMS statement.
- The TCPCONFIG statement instead of the KEEPALIVEOPTIONS statement. The TCPCONFIG statement provides support for the parameters currently on the KEEPALIVEOPTIONS statement.
- NPF (Network Print Facility) was previously shipped in a separate FMID. In z/OS V1R4 Communications Server, NPF is merged into the base. This change will not affect your operations.
- In order to prevent abends when the TCP/IP stack is run with an out of date version of the message catalog, the TCP/IP stack now will verify that the message catalog is current. The TCP/IP stack will revert to issuing default messages when it determines that the message catalog is out-of-date or inaccessible. This change allows TCP/IP to continue processing even without a message catalog.
- The limit on the number of RCPTs in a single SMTP job is 3000. If you have more than 3000 RCPTs in a single SMTP job, the excessive RCPT commands will receive a failure reply code '552 Too many recipients'. Abend B37 can still occur if no more space is available on volume or if the volume table of contents (VTOC) is full.

Sysplex Distributor enhancements

In z/OS CS V1R4, Sysplex Distributor is enhanced in the following three areas:

- “Sysplex-wide Dynamic Source VIPAs for TCP connections”
- “Sysplexports” on page 67
- “Sysplex Wide Security Association (SWSA)” on page 68

Sysplex-wide Dynamic Source VIPAs for TCP connections

For clients outside a Parallel Sysplex, Sysplex Distributor provides a single-IP-address appearance to application instances spread across the Sysplex. It also distributes incoming work among the various instances. Many applications are part of a cooperative network of applications, and the Sysplex applications that serve as clients to end users may also have to initiate (client-like) outbound connection requests to cooperating applications. The SOURCEVIPAs feature allows applications to attain independence of any physical adapter; however, SOURCEVIPAs is limited to statically defined VIPAs within a stack. Different instances of the same application using Sysplex Distributor, and thus having a single IP address for inbound connection requests, will use different IP addresses for their outbound connection requests. These problems are resolved by allowing a Dynamic VIPA (DVIPA) to be used as the source IP address for TCP applications and to have the Sysplex stacks collaborate on assigning ephemeral ports to prevent duplicate connection 4-tuples when the same Distributed DVIPA is used as the source address on multiple stacks. (The term *4-tuples* here refers to the source IP address, the source port, the destination IP address, and the destination port.) These solutions are provided in z/OS CS V1R4 by Sysplex-wide Dynamic Source VIPAs for TCP connections and Sysplexports.

This enhancement is made possible by a new configuration option, TCPSTACKSOURCEVIPAs, that specifies an IPv4 address to be used as the local address for all outbound TCP connections if a bind() has not been issued for the socket.

The Dynamic VIPA address specified on the new TCPSTACKSOURCEVIPA can be created by a VIPADEFINE, created within a VIPARANGE, or created as a result of being a target stack for Sysplex Distributor.

Restrictions

TCPSTACKSOURCEVIPA support is for TCP connections only.

What this change affects

- Application development
- Customization
- Operations
- Usability

Migration procedures

If you want to take advantage of the Sysplex-wide Dynamic Source VIPAs for TCP connections enhancement, perform the task in the following table.

Table 29. Sysplex-wide Dynamic Source VIPAs for TCP connections - Migration task

Task	Procedure	Reference
Enable the TCPSTACKSOURCEVIPA function.	Code SOURCEVIPA and TCPSTACKSOURCEVIPA in the IPCONFIG statement specifying the desired source IP address.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Sysplexports

Sysplex Distributor is enhanced with a facility to allow assignment of ephemeral ports for outbound connections to be managed across the entire Sysplex, such that for a particular Distributed DVIPA, a particular port value is assigned to a socket on only one TCP stack in the Sysplex. This will ensure that inbound connection data can always be uniquely routed to the correct application instance, whether the connection was initiated by the client or by the Sysplex application instances.

This enhancement is made possible by a new configuration option, SYSPLEXPORTS, on the VIPADISTRIBUTE statement.

Restrictions

Sysplex-wide ephemeral port assignment applies only to Distributed DVIPAs, and not to other kinds of Dynamic VIPAs.

Performance issues

Due to the additional overhead caused by having to access the coupling facility during both obtaining or reserving an ephemeral port during socket connect() processing and returning the port during socket close() processing, there will be a performance degradation if this function is for short-lived connections (such as Web traffic). For longer-lived connections (such as FTP transfers and TN3270 sessions), the coupling facility overhead is minimal in comparison to the overall connection time; therefore, there is negligible performance degradation for these connection types.

What this change affects

- Application development
- Customization
- Operations
- Usability

Migration procedures

If you want to take advantage of the Sysplexports enhancement, perform the task in the following table.

Table 30. Sysplexports - Migration task

Task	Procedure	Reference
Enable Sysplexports allocation.	Perform the following steps: <ul style="list-style-type: none">• Set up the EZBEPOR Coupling Facility Structure.• Code the SYSPLEXPORTS keyword on a VIPADISTRIBUTE statement.	<i>z/OS Communications Server: SNA Network Implementation Guide, z/OS Communications Server: IP Configuration Reference, and z/OS Communications Server: IP Configuration Guide</i>

Sysplex Wide Security Association (SWSA)

Sysplex Wide Security Association (SWSA) extends the use of IPSec tunnels in a sysplex environment. It is available for Dynamic VIPA takeover and for Sysplex Distributor.

For Dynamic VIPA takeover and giveback, SWSA does the following:

- It allows the IPSec tunnel information to move with the Dynamic VIPA instead of terminating the tunnel.

For Sysplex Distributor, SWSA does the following:

- It allows the IPSec tunnel information to be distributed to the target host, creating end-to-end security.
- It allows the cryptography processing done by IPSec to be distributed to target hosts, thus removing this burden from the distributor host.

Restrictions

The following restrictions apply:

- The distribution of IPSec tunnels with Sysplex Distributor requires the IPSec policy for the dynamic VIPA address to be defined at a connection or host based granularity.
- Specifying a subnet or range granularity is not supported.
- The distributor host and any backups must be at the z/OS V1R4 CS level and only target hosts that are at the z/OS V1R4 CS level are eligible for distributed IPSec tunnel traffic.
- All systems that are participating (distributor and targets) in IPSec traffic distribution must be running the same FMID level code.
- This feature does not apply to manual tunnels.

What this change affects

- Security
- Availability

Migration procedures

If you want to take advantage of the SWSA function, perform the task in the following table.

Table 31. Sysplex Wide Security Association (SWSA) - Migration task

Task	Procedure	Reference
Enable IPsec tunnels to be moved during VIPA takeover or giveback and allow IPsec traffic to be distributed in a Sysplex Distributor environment.	Perform the following steps: <ol style="list-style-type: none"> 1. Define an EZBDVIPA structure in the CFRM policy and activate the policy. 2. In the TCP/IP profile, code the DVIPSEC subparameter on the FIREWALL parameter in the IPCONFIG statement. 3. Ensure that your IPsec policy is defined to be identical on any host that may take over the dynamic VIPA or that may be a target for a Sysplex Distributed workload. 	<i>z/OS Communications Server: IP Configuration Reference</i> , <i>z/OS Communications Server: IP Configuration Guide</i> , and <i>z/OS Communications Server: SNA Network Implementation Guide</i>

Access control for network and Fast Response Cache Accelerator (FRCA)

Network access control

z/OS V1R4 CS extends the network access control function first provided in CS for OS/390 V2R10 (see “Network access control” on page 150). Permission for users to access certain networks and resources may now be checked inbound as well as outbound. This ensures that network access privileges are checked prior to applications receiving any data for processing. Following changes to the SERVAUTH class, the NetAccess zone table must be reloaded to cause the stack to recognize the change for existing connections.

A new ioctl service is provided through z/OS UNIX System Services and it returns Port of Entry information about the peer address associated with a socket suitable for use with RACROUTE VERIFY processing.

New parameters are provided on the NETACCESS statement in the TCPIP PROFILE for activating inbound checking.

Restrictions

A security product that supports the SERVAUTH class, such as z/OS Security Server (RACF), is required for use of this function. The SERVAUTH class must be RACLISTed and the user IDs that clients or servers run under must be permitted to the resource names that protect each network.

If you define or modify a net access resource after a socket is in use, you must replace the TCPIP PROFILE net access zone table to cause the TCP/IP stack to recognize the resource profile change on that socket. Refer to the Network Access Control section in *z/OS Communications Server: IP Configuration Guide* for details.

What this change affects

- Customization
- Operation
- Diagnosis
- System Security

Migration procedures

If you want to take advantage of the network access control enhancement, perform the tasks in the following table.

Table 32. Network access control - Migration tasks

Task	Procedure	Reference
Activate Network Access Control Inbound.	Add an INBOUND parameter to the NETACCESS statement in TCPIP PROFILE.	<i>z/OS Communications Server: IP Configuration Guide</i>
Notify the TCP/IP stack of changes to SERVAUTH class.	RACLIST or REFRESH the SERVAUTH class. Reconfigure the net access security zone table with an OBEY file.	<i>z/OS Communications Server: IP Configuration Guide</i>

Fast Response Cache Accelerator (FRCA) access control

FRCA access control is a new z/OS CS V1R4 security function that allows control of access to the TCP/IP stack FRCA services by a Web server application using a security product, such as the z/OS Security Server (RACF). This allows you to control which user IDs may use the FRCA service. This function is provided by way of a new Access Facility (SAF) resource in the SERVAUTH class.

Restrictions

FRCA access control is not applicable to TCP/IP releases prior to z/OS CS V1R4. In addition, a security product that supports the SERVAUTH class, such as z/OS Security Server (RACF), is required for use of this function. The SERVAUTH class must be RACLISTed and the user IDs that servers run under must be permitted to the resource name that protects the FRCA service.

If the security product indicates that the FRCA access resource profile is *not* defined, access will be allowed.

What this change affects

- Customization
- Diagnosis
- System Security

Migration procedures

If you want to take advantage of the FRCA access control enhancement, perform the tasks in the following table. No action is required to keep your system working the way it previously worked without the definition.

Table 33. FRCA access control - Migration tasks

Task	Procedure	Reference
Configure the security product for FRCA access control.	Define the SAF resource profile for FRCA access in the SERVAUTH class.	<i>z/OS Communications Server: IP Configuration Guide</i>
Authorize a Web server to use FRCA services.	Permit the user ID the Web server runs under to the FRCA resource.	<i>z/OS Communications Server: IP Configuration Guide</i>

Resolver enhancements

In z/OS CS V1R4, the local host table processing of the resolver was modified to introduce:

- A new type of local host table, IPNODES.
- Changes to the local host table search order.

- A new optional resolver setup statement to specify a global IPNODES table containing IP address to IP host name mapping. This allows an installation to consolidate this information.
- A new optional resolver setup statement to specify a default IPNODES table containing IP address to IP host name mapping. This allows an installation to provide default information in the event that an individual user does not maintain a private local host table.
- A new optional resolver setup statement to specify that the same local host table search order is to be used for resolver queries in both the native MVS and the z/OS UNIX environments.

Refer to *z/OS Communications Server: IP Configuration Guide* for information about the new local host table and search order. Refer to *z/OS Communications Server: IP Configuration Reference* for information about the new resolver setup statements. See “IPv6 support for the resolver” on page 82 for updates that were made to the resolver specifically for IPv6 support.

Restrictions

None.

What this change affects

- Application Development

Migration procedures

If you want to take advantage of the resolver enhancements, perform the desired tasks in the following table.

Table 34. Resolver enhancements - Migration tasks

Task	Procedure	Reference
Change the location of the global and default IPNODES files.	Create new global and default IPNODES files and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	<i>z/OS Communications Server: IP Configuration Reference</i>
Reread existing global and default IPNODES files.	Update existing global and default IPNODES files and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	<i>z/OS Communications Server: IP Configuration Reference</i>
Use the common search order for native MVS and the z/OS UNIX environments.	Add a new statement COMMONSEARCH in the resolver setup and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Use the Getaddrinfo and Getnameinfo services information query.	Ensure that the MVS services information data set (ETC.SERVICES) is fixed (F) or fixed block (FB) with a logical record length (LRECL) between 56 and 256.	<i>z/OS Communications Server: IP Configuration Guide</i>

Managed System Infrastructure (msys) for Setup enhancement

msys for Setup was introduced in z/OS CS V1R2; see “Managed System Infrastructure (msys) for Setup” on page 123 for details. In z/OS CS V1R4, msys for Setup support was enhanced to include configuring a TN3270 Server and IP port reservations.

Restrictions

None.

What this change affects

- Customization
- Diagnosis
- System Security

Migration procedures

To take advantage of msys for Setup enhancement, perform the task shown in Table 70 on page 124. Note that all configuration data saved in LDAP using msys for Setup support from a previous release is preserved and automatically migrated to the z/OS CS V1R4 level.

OSA SNMP subagent support

For several releases, Communications Server has supported OSA adapter SNMP network management data defined in the IBM MVS Enterprise-specific MIB for some OSA adapters. With z/OS CS V1R4, the new SNMP subagent and OSA MIB provided by the OSA product can be used with the Communications Server SNMP support to provide SNMP management data for some OSA adapters. The OSA adapter management data defined in the Communications Server IBM MVS Enterprise-specific MIB will continue to be supported. Refer to *zSeries: OSA-Express Customer's Guide and Reference* for details regarding the OSA SNMP subagent and OSA MIB.

Restrictions

None.

What this change affects

- SNMP network management

Migration procedures

There are no z/OS CS V1R4 migration tasks for the OSA subagent support.

Event trace enhancements

In z/OS CS V1R4, the event trace functions are enhanced in the following ways:

- IPv6 addresses can be specified on the IPADDR trace option keyword to execute traces on IPv6 addresses. See “IPv6 support for event trace enhancements” on page 86 for the migration procedure.
- Captured traces can be further analyzed in a variety of ways by using IPCS.
- Support is added for IPv4 address prefix.
- The SOCKAPI event trace option was removed from the 'ALL' group option.
- A new event trace option called ND is added for the z/OS CS V1R4 Neighbor Discovery function.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

If you want to take advantage of the event trace enhancements, perform the tasks in the following table.

Table 35. Event trace enhancements - Migration tasks

Task	Procedure	Reference
Filter the TCPIP event trace by a group of IPv4 addresses using an address prefix.	Append a slash followed by a numeric value (in the range of 1-32) for the IPv4 address prefix on the IPv4 address filter specified in either a SYS1.PARMLIB member or in a Trace CT command. For example, 192.48.32/24 allows addresses from 192.48.32.00 to 192.48.32.255 to be filtered.	<i>z/OS Communications Server: IP Diagnosis</i>
Turn on the Neighbor Discovery (ND) trace option.	Add ND to the list of trace options to the component trace SYS1.PARMLIB member. This turns on the ND trace option at TCP/IP initialization. Issue a Trace CT command with OPTIONS=(ND) to turn on the ND trace option after TCP/IP initialization.	<i>z/OS Communications Server: IP Diagnosis</i>

TCP/IP support for Simple Network Time Protocol (SNTP)

TIMED is a TCP/IP daemon that is used to provide the time. TIMED gives the time in seconds since midnight January 1, 1900. SNTPD is a new TCP/IP daemon that is also used to provide the time in order to synchronize a network of (S)NTP clients. Simple network time protocol provides for a more accurate time. SNTPD does not replace TIMED but it is the preferred server for synchronizing time in the network.

Restrictions

The following restrictions apply:

- The SNTP daemon does not support IPv6.
- SNTP uses the same time-request/reply format that NTP does. It does not support any of the management functions of the NTP protocol.
- According to the SNTP RFC 2030, it is appropriate to use an SNTP server at the root of the time synchronization tree (stratum 1), which is where an OS/390 or z/OS system would be located. The ETR (external time reference) is stratum 0. Therefore, the ETR clock cannot be changed by SNTP.

Dependencies

To use SNTPD, UNIX System Services must be active and TCP/IP must be started.

What this change affects

- Operations
- Usability

Migration procedures

If you want to take advantage of the TCP/IP support for SNTP, perform the task in the following table.

Table 36. TCP/IP support for Simple Network Time Protocol (SNTP) - Migration task

Task	Procedure	Reference
Synchronize (S)NTP clients with the ETR as the source.	<p>Do the following:</p> <ol style="list-style-type: none"> 1. Read and understand the SNTP chapters in <i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>. 2. Start SNTPD. Note that when restricting low port usage, the port used by SNTPD (default value of 123) should either be reserved for the name of the SNTPD start procedure or the PORT statement's SERVAUTH Security Access Facility (SAF) parameter used. 3. Be aware that time is broadcasted/multicast to (S)NTP clients or unicast to clients if requested by the client. 	<p><i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i></p>

Netstat enhancements

In z/OS CS V1R4, Netstat is changed in the following ways:

- It displays the IP configuration setting with the value of Yes or No instead of the value of 00001 or 00000.
- The new INTFName/-K filter is added to DEVLINKS/-d report to provide the response on the specified link or interface name.
- The Netstat ALL/-A, BYTEINFO/-b, and TELNET/-t reports are enhanced to support 64-bit counters when a long format report is requested.
- For TSO NETSTAT, when a long format report is requested, no message identifiers are displayed in the output for those reports that have been modified for IPv6 support. If you have developed REXX programs that issue the Netstat command under TSO and parse the output lines based on message identifiers, refer to the TSO NETSTAT command output parsing consideration in *z/OS Communications Server: IP System Administrator's Commands* for more information.
- The following output control options are now available:

FORMAT/-M SHORT

Displays the output in the existing IPv4 format.

FORMAT/-M LONG

Displays the output in the format that supports IPv6 addresses.

These output control options allow the stack to be configured for IPv4-only operation (not IPv6-enabled), while still allowing you to modify programs that rely on Netstat output to update and test new versions of these programs with IPv6-enabled output from Netstat.

- A stack-wide output format parameter (FORMAT SHORT/LONG) can be specified on the IPCONFIG profile statement. It will instruct Netstat to produce output in one of the above formats. FORMAT SHORT is only applicable when the stack is not IPv6-enabled.
- In addition to the stack-wide FORMAT parameter, a Netstat command line option FORMAT/-M with keyword SHORT/LONG is supported to override the stack-wide parameter. Whenever a user specifies the Netstat command line format option, it will override the stack-wide format parameter on an IPv4-only stack.

See “IPv6 support for Netstat” on page 84 for updates that were made to Netstat specifically for IPv6 support. Refer to *z/OS Communications Server: IP System Administrator’s Commands* for a complete description of the Netstat command.

Restrictions

None.

What this change affects

- Usability

Migration procedures

There are no migration procedures other than noting the changed configuration setting’s value.

Ping enhancements

The TSO PING command is converted to a UNIX C socket application and now supports all the input parameters that are supported by the UNIX shell oping/ping command. As a UNIX application, TSO PING may be affected by environment variables settings. Refer to *z/OS Communications Server: IP System Administrator’s Commands* for a complete description of these commands.

For TSO PING, the following changes affect command processing and output:

- The old messages previously issued by TSO PING are no longer issued. Some of the messages issued by the new TSO PING will be the same as those now issued by the UNIX shell oping/ping command. Other new messages are added.
- Message identifiers are no longer associated with the TSO PING output. For example, in prior releases, if MSGID was in effect for the TSO PROFILE, the TSO PING output would appear with the following message identifiers:

```
EZA0458I Ping CS V1R4: Pinging host 9.67.113.43. Use ATTN to interrupt.  
EZA0463I PING: Ping #1 response took 0.002 seconds. Successes so far 1.
```

As of this release, the output for this same TSO PING command appears without message identifiers, even if MSGID was in effect for the TSO PROFILE :

```
Ping CS V1R4: Pinging host 9.67.113.43. Use ATTN to interrupt.  
PING: Ping #1 response took 0.002 seconds. Successes so far 1.
```

Message identifiers for informational and error messages are still supported and are displayed based on the TSO PROFILE MSGID setting.

- For TSO PING to be authorized to use RAW sockets, you must update member IKJTSOxx in SYS1.PARMLIB by adding PING under AUTHCMD NAMES

For UNIX shell oping/ping, some new messages may be issued.

The TSO PING and UNIX shell oping/ping commands are enhanced in z/OS CS V1R4 to support IPv6 IP addresses. See “IPv6 support for Ping” on page 85 for more information.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Migration procedures

If you want to take advantage of the Ping enhancements, perform the tasks in the following table.

Table 37. Ping enhancements - Migration tasks

Task	Procedure	Reference
Utilize new input parameters for TSO PING command.	Specify PING with new input parameters.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Update any automated applications that expect certain message identifiers from the TSO PING command responses.	Remove any verification of message identifiers for PING output. Update any verification of message identifiers for informational or error messages to use new message identifiers. If desired, add support for new messages.	<i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>

Traceroute enhancements

In z/OS CS V1R4, the TSO TRACERTE command is converted to a UNIX application and it now supports all the input parameters supported by the UNIX shell otracert/traceroute command.

As a UNIX application, TSO TRACERTE may be affected by environment variables settings. Furthermore, the default destination port number is changed from 4096 to 33434. Refer to *z/OS Communications Server: IP System Administrator's Commands* for a complete description of these commands.

For TSO TRACERTE, the following changes affect command processing and output:

- In prior releases, TSO TRACERTE only used the HOSTS.ADDRINFO file for IP address to host name resolution for the IP addresses in received ICMP responses. As of z/OS CS V1R4, TSO TRACERTE may use a DNS along with the local host tables. For more information about the local host tables, refer to *z/OS Communications Server: IP Configuration Guide*.
- The old messages previously issued by TSO TRACERTE are no longer issued. Some of the messages issued by the new TSO TRACERTE will be the same as those now issued by the UNIX shell otracert/traceroute command. Other new messages are added.
- Message identifiers are no longer associated with the TSO TRACERTE output. For example, in prior releases, if MSGID was in effect for the TSO PROFILE, the TSO TRACERTE output would appear with the following message identifiers:

```
tracerte 129.35.130.09
EZA0484I Trace route to 129.35.130.09 (129.35.130.9)
EZA0505I 1 (9.67.22.2) 61 ms 62 ms 56 ms
EZA0505I 2 * * *
EZA0505I 3 (9.67.1.5) 74 ms 73 ms 80 ms
EZA0505I 4 (9.3.8.1) 182 ms 200 ms 184 ms
EZA0505I 5 (129.35.208.2) 170 ms 167 ms 163 ms
EZA0505I 6 * (129.35.208.2) 192 ms !H 157 ms !H
EZA0516I
```

As of this release, the output for this same TSO TRACERTE command appears without message identifiers, even if MSGID was in effect for the TSO PROFILE :

```
tracerte 129.35.130.09
CS V1R4: Traceroute to 129.35.130.09 (129.35.130.9)
 1 (9.67.22.2) 61 ms 62 ms 56 ms
 2 * * *
 3 (9.67.1.5) 74 ms 73 ms 80 ms
 4 (9.3.8.1) 182 ms 200 ms 184 ms
 5 (129.35.208.2) 170 ms 167 ms 163 ms
 6 * (129.35.208.2) 192 ms !H 157 ms !H
```

Message identifiers for informational and error messages are still supported and are displayed based on the TSO PROFILE MSGID setting.

For UNIX shell otracert/traceoute, most of the existing messages have been changed and some new messages may be issued. For example, the text *otracer*: has been removed from the existing messages since some of these messages will now also be used by TSO TRACERTE.

The TSO TRACERTE and UNIX shell otracert/traceroute commands are enhanced in z/OS CS V1R4 to support IPv6 IP addresses. See “IPv6 support for Traceroute” on page 85 for more information.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Migration procedures

If you want to take advantage of the Traceroute enhancements, perform the tasks in the following table.

Table 38. Traceroute enhancements - Migration tasks

Task	Procedure	Reference
Utilize new input parameters for TSO TRACERTE command	Specify TRACERTE with new input parameters.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Update any automated applications that expect certain message text from the TSO TRACERTE command responses.	Remove any verification of message identifiers for TRACERTE output. Update any verification of message identifiers for informational or error messages to use new message identifiers. If desired, add support for new messages.	<i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>
Update any automated applications that expect certain message identifiers or message text from the otracert or traceroute commands.	Update any verification of message identifiers or message text for informational or error messages. If desired, add support for new messages.	<i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>

New VTAM start options to adjust the QDIO or iQDIO storage

The amount of storage used for read processing for both QDIO and iQDIO (HiperSockets) devices has been increased. In the tables below, the "New value" columns show the new defaults. The "Old value" columns indicate the previously existing amount of storage, which can be calculated against the new value to determine the storage increase. The increases are on a per active data device basis.

OSA Express storage for read processing

Table 39. OSA Express: Amount of storage for read processing

	Old value	New value
zSeries (64 bit)	.5 meg	4 meg
non 64 bit	.5 meg	1 meg

HiperSockets storage for read processing

Table 40. HiperSockets: Amount of storage for read processing

CHPID MFS	Old value	New value
64k	4 meg	8 meg
40k	4 meg	5 meg
24k	3 meg	3 meg (no change)
16k	2 meg	2 meg (no change)

As a result of this increase, two new VTAM start options allow you to adjust the QDIO or iQDIO storage used for each data device (read processing). The options are global, which means that they affect all QDIO or iQDIO devices. For most users, the defaults of these start options are appropriate, and you will probably never have to change them. However, there are valid configurations (such as many OSA adapters, or multiple TCP/IP stacks per LPAR, or many 2nd level guests) in which you may need to adjust this storage.

The new options are as follows:

- The QDIOSTG (QDIO Storage) option allows you to define how much storage VTAM keeps available for read processing for all OSA QDIO data devices.
- The IQDIOSTG (iQDIO Storage) option allows you to define how much storage VTAM keeps available for read processing for all HiperSockets (iQDIO) data devices that use a MFS (Maximum Frame Size) of 64k.

Refer to *z/OS Communications Server: SNA Migration* for more information regarding these new VTAM start options, including sample displays. Refer to *z/OS MVS Initialization and Tuning Reference* for information about reviewing and altering the IVTPRM00 parmlib member for CSM fixed storage. Refer to *SNA Resource Definition Reference* Information APAR ii13235 for additional CSM information.

Note: This function is being made available in z/OS CS V1R2 by APAR OW52291.

Restrictions

None.

What this change affects

- Storage for read processing

Migration procedures

The defaults of the new storage options will be appropriate for most users; however, IBM recommends that all users perform the first task in the following table. The second and third tasks are necessary only if you determine that you need to change the storage options.

Table 41. New VTAM start options to adjust the QDIO or iQDIO storage - Migration tasks

Task	Procedure	Reference
Recommended: Review CSM specifications for fixed CSM storage.	Review (and alter if necessary) the IVTPRM00 parmlib member for CSM fixed storage.	Refer to <i>z/OS MVS Initialization and Tuning Reference</i> and refer to <i>SNA Resource Definition Reference Information APAR ii13235</i> for additional CSM information.
Optionally: Define how much storage VTAM keeps available for read processing for all OSA QDIO data devices.	Code the QDIOSTG (QDIO Storage) start option.	<i>SNA Resource Definition Reference Information APAR ii13235</i>
Optionally: Define how much storage VTAM keeps available for read processing for all HiperSockets (iQDIO) data devices that use a MFS (Maximum Frame Size) of 64k.	Code the IQDIOSTG (iQDIO Storage) start option.	<i>SNA Resource Definition Reference Information APAR ii13235</i>

IPv6 support

Enabling IPv6 support

In previous releases, the TCP/IP stack supported only IPv4 addresses. z/OS CS V1R4 supports both IPv4 and IPv6 IP addresses. If you want to use IPv6 support, you must first enable the TCP/IP stack for IPv6 processing by tailoring your BPXPRMxx member.

Migration considerations

Consider the following as you migrate:

- CS for OS/390 V2R10 introduced some limited IPv6 support for TCP/IP applications. This limited IPv6 support was also enabled by using the NETWORK statement in the BPXPRMxx parmlib member. As a result, if you had previously enabled this feature, no additional action is required to enable the IPv6 support introduced in z/OS CS V1R4.

Note: Any Communications Server TCP/IP applications that are now IPv6 capable (such as Netstat and FTP) will begin using IPv6 services when you migrate to this release.

- The limited IPv6 support of AF_INET6 in the BPXPRMxx NETWORK statement in CS for OS/390 V2R10 was only at the TCP/IP layer. This means that the following was true in CS for OS/390 V2R10:
 - The stack was not IPv6 enabled.
 - The Netstat reports were unchanged.
 - No IPv6 interfaces were defined.

- Only IPv4-mapped addresses were supported on API calls.
- No new IPv6 APIs were supported.

In z/OS CS V1R4, the behavior of the AF_INET6 in the BPXPRMxx NETWORK statement is changed. If you have it coded, the following is true in z/OS CS V1R4:

- The stack is IPv6 enabled.
- All Netstat reports will be in the new (long) format.
- At a minimum, the IPv6 LOOPBACK interface will be enabled.
- IPv6 addresses will be reported.
- IPv6 APIs are supported.

Restrictions

None.

What this change affects

- IPv6 application enablement and communication

Migration procedures

If you want to enable IPv6 address support, perform the task in the following table.

Table 42. Enabling IPv6 support - Migration task

Task	Procedure	Reference
Enable TCP/IP for IPv6 by tailoring your BPXPRMxx SYS1.PARMLIB member.	Add an AF_INET6 NETWORK statement to your BPXPRMxx member.	<i>z/OS Communications Server: IPv6 Network and Application Design Guide</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Configuration changes related to IPv6 support

Some existing command parameters are modified for IPv6. Other parameters are introduced in this release to accommodate functions that are new with the IPv6 support. These new parameters are configured under a new statement called IPCONFIG6.

Specifically, these are new or changed configuration statements:

- BEGINROUTES (changed)
- DELETE PORT (changed)
- INTERFACE (new)
- IPCONFIG (changed and updated with new FORMAT keyword)
- IPCONFIG6 (new)
- PKTTRACE (changed)
- PORT (changed)

The changed operator commands include the following:

- V TCPIP,,DATTRACE
- V TCPIP,,PKTTRACE

See the tables in Chapter 3, “New and changed interfaces” on page 29 for information about the changes to statements and commands from release to release. Refer to *z/OS Communications Server: IP Configuration Guide* and to *z/OS Communications Server: IPv6 Network and Application Design Guide* for detailed

discussion about IPv6 configuration considerations. Refer to *z/OS Communications Server: IP Configuration Reference* for details on the syntax of statements, parameters, and commands.

Restrictions

In order to use IPv6 support, the stack must be configured for IPv6.

Incompatibilities

The following configuration statements will be rejected if the stack is not configured for IPv6:

- BEGINROUTE ROUTEs with IPv6 addresses coded
- DELETE PORT statements with IPv6 BIND addresses coded
- INTERFACE
- IPCONFIG6
- PORT statements with IPv6 BIND addresses coded
- PKTTRACE statements that have IPv6 addresses

Dependencies

IPv6 must be enabled before IPv6 addresses can be coded on the configuration statements.

Migration procedures

If you want to use IPv6 address support, perform the configuration tasks in the following table.

Table 43. Configuration changes related to IPv6 support - Migration tasks

Task	Procedure	Reference
Add an IPv6 route to the IP route table.	Specify BEGINROUTES with an IPv6 address.	<i>z/OS Communications Server: IP Configuration Reference</i>
Control packet tracing for IPv6 address.	Specify one of the following with an IPv6 address: <ul style="list-style-type: none"> • PKTTRACE statement • V TCPIP,,PKTTRACE command 	<i>z/OS Communications Server: IP Configuration Reference</i>
Trace socket data for IPv6 address.	Specify V TCPIP,,DATTRACE with an IPv6 address.	<i>z/OS Communications Server: IP Configuration Reference</i>
If the stack is not enabled for IPv6, display command output as if it could contain IPv6 addresses.	Specify IPCONFIG FORMAT LONG.	<i>z/OS Communications Server: IP Configuration Reference</i>
Enable IPv6 forwarding.	Specify IPCONFIG6 DATAGRAMFWD.	<i>z/OS Communications Server: IP Configuration Reference</i>
Enable multipath route selection for IPv6.	Specify IPCONFIG6 MULTIPATH PERPACKET or IPCONFIG6 MULTIPATH PERCONNECTION.	<i>z/OS Communications Server: IP Configuration Reference</i>
Ignore ICMPv6 redirects.	Specify IPCONFIG6 IGNOREREDIRECT.	<i>z/OS Communications Server: IP Configuration Reference</i>
Enable IPv6 Source VIPA support.	Specify IPCONFIG6 SOURCEVIPA and code the SOURCEVIPAIN keyword on an IPv6 INTERFACE statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Set IPv6 hop limit.	Specify IPCONFIG6 HOPLIMIT.	<i>z/OS Communications Server: IP Configuration Reference</i>
Set IPv6 ICMP error limit.	Specify IPCONFIG6 ICMPERRORLIMIT.	<i>z/OS Communications Server: IP Configuration Reference</i>

Table 43. Configuration changes related to IPv6 support - Migration tasks (continued)

Task	Procedure	Reference
Ignore hop limit options in Router Advertisement messages that are received.	Specify IPCONFIG6 IGNOREROUTERHOPLIMIT.	<i>z/OS Communications Server: IP Configuration Reference</i>
Configure IPv6 interfaces.	Specify INTERFACE DEFINE.	<i>z/OS Communications Server: IP Configuration Reference</i>
Delete IPv6 interfaces.	Specify INTERFACE DELETE.	<i>z/OS Communications Server: IP Configuration Reference</i>
Add an IPv6 address to an existing INTERFACE definition.	Specify INTERFACE ADDADDR.	<i>z/OS Communications Server: IP Configuration Reference</i>
Delete IPv6 address from existing INTERFACE definition.	Specify INTERFACE DELADDR.	<i>z/OS Communications Server: IP Configuration Reference</i>
Deprecate an IPv6 address that was configured manually.	Specify INTERFACE DEPRADDR.	<i>z/OS Communications Server: IP Configuration Reference</i>
Associate a job with an IPv6 address and bind that job's listening sockets to that address.	Specify PORT with an IPv6 address for the BIND option.	<i>z/OS Communications Server: IP Configuration Reference</i>

IPv6 support for the resolver

In z/OS CS V1R4, IPv6 support introduces several changes to how host name and IP address resolution is performed. These changes affect several areas of resolver processing:

- New resolver APIs are introduced for IPv6 enabled applications.
The new APIs, Getaddrinfo and Getnameinfo, allow applications to query host names for IPv6-enabled hosts and IPv6 addresses. The APIs also allow the application to optionally query a server's port and protocol. These APIs also allow the application to optionally query a server's port and protocol. A third new API, Freeaddrinfo, works in conjunction with Getaddrinfo to provide a thread safe environment.
Refer to the discussion on resolver enhancements in *z/OS Communications Server: IPv6 Network and Application Design Guide* for more information.
- New DNS resource records are defined to represent hosts with IPv6 addresses. This changes the contents of network flows between resolvers and name servers.
See Chapter 12, "Migrating to the BIND-based DNS name server" on page 249 for more information about the DNS IPv6 support.
- The resolver uses an RFC defined algorithm to sort addresses returned for a multi-homed host.
Refer to the discussion on Default Address selection-Destination address selection in *z/OS Communications Server: IPv6 Network and Application Design Guide* for information about the sorting algorithm utilized by the resolver's Getaddrinfo processing.
- New local host table support. This introduces:
 - A new type of local host table, IPNODES.
 - Changes to the local host table search order.

- A new optional resolver setup statement to specify a global IPNODES table containing IP address to IP host name mapping. This allows an installation to consolidate this information.
- A new optional resolver setup statement to specify a default IPNODES table containing IP address to IP host name mapping. This allows an installation to provide default information in the event that an individual user does not maintain a private local host table.
- A new optional resolver setup statement to specify that the same local host table search order is to be used for both IPv4 and IPv6 queries.

Refer to *z/OS Communications Server: IP Configuration Guide* for information about the new local host table and search order. Refer to *z/OS Communications Server: IP Configuration Reference* for information about the new resolver setup statements.

Restrictions

None.

What this change affects

- Application Development

Migration procedures

If you want to take advantage of the IPv6 support for resolver, perform the desired tasks in the following table.

Table 44. IPv6 support for resolver - Migration tasks

Task	Procedure	Reference
Change the location of the global and default IPNODES files.	Create new global and default IPNODES files and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	<i>z/OS Communications Server: IP Configuration Reference</i>
Reread existing global and default IPNODES files.	Update existing global and default IPNODES files and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	<i>z/OS Communications Server: IP Configuration Reference</i>
Use the common search order of IPv4 and IPv6 name query.	Add a new statement COMMONSEARCH in the resolver setup and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Use the Getaddrinfo and Getnameinfo services information query.	Ensure that the MVS services information data set (ETC.SERVICES) is fixed (F) or fixed block (FB) with a logical record length (LRECL) between 56 and 256.	<i>z/OS Communications Server: IP Configuration Guide</i>

IPv6 support for applications

The following applications support IPv6:

- FTP server and FTP client – see “IPv6 support for FTP” on page 180 for more information.
- Inetd server
- Otelnetd server
- Orshd server
- Orexecd server
- UNIX rexec client
- Netstat – see “IPv6 support for Netstat” on page 84 for more information.
- TSO/UNIX Traceroute – see “IPv6 support for Traceroute” on page 85 for more information.

- TSO/UNIX Ping – see “IPv6 support for Ping” on page 85 for more information.

Restrictions

None.

What this change affects

- Usability

Migration procedures

Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for complete information on using the new IPv6 support for these applications.

IPv6 support for Netstat

In z/OS CS V1R4, the following updates are made to Netstat for IPv6 support:

- The Netstat command now supports IPv6 IP addresses and displays IPv6 related information.
- A stack-wide output-format parameter (FORMAT SHORT/LONG) can be configured on the IPCONFIG profile statement. It can be used to instruct Netstat to produce output according to the old format or the new format. FORMAT SHORT is only applicable when the stack is not IPv6-enabled.
- A new Netstat FORMAT/-M option with keyword SHORT/LONG is supported. It can be used to override the stack-wide parameter.
- The Netstat ALL/-A, BYTEINFO/-b, and TELNET/-t reports are enhanced to support 64-bit counters.
- The Netstat IP address filter is enhanced to support IPv6 IP addresses.
- For TSO NETSTAT, if the command is issued from an IPv6-enabled stack or if the command is issued from an IPv4-only stack but the request is for a long format display, no message identifiers are displayed in the output. Refer to the TSO NETSTAT command output parsing considerations in *z/OS Communications Server: IP System Administrator's Commands* for more information for users who have developed REXX programs that issue Netstat command under TSO and parse the output lines based on message identifiers.

See “Netstat enhancements” on page 74 for updates to Netstat in z/OS CS V1R4 that are not related to IPv6 support. Refer to *z/OS Communications Server: IP System Administrator's Commands* for a complete description of the Netstat command.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Migration procedures

If you want to take advantage of the IPv6 support for Netstat, perform the task in the following table.

Table 45. IPv6 support for Netstat - Migration task

Task	Procedure	Reference
View TCP/IP information by using Netstat.	Specify the appropriate Netstat command with desired options.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

IPv6 support for Ping

The TSO PING and UNIX shell oping/ping commands are enhanced in z/OS CS V1R4 to support IPv6 IP addresses. Refer to *z/OS Communications Server: IP System Administrator's Commands* for a complete description of these commands.

See “Ping enhancements” on page 75 for updates to Ping in z/OS CS V1R4 that are not related to IPv6 support.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Migration procedures

If you want to take advantage of the IPv6 support for Ping, perform the tasks in the following table.

Table 46. IPv6 support for Ping - Migration tasks

Task	Procedure	Reference
Exploit the Ping IPv6 support.	Specify IPv6 host names or IP addresses on the Ping command options.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

IPv6 support for Traceroute

The TSO TRACERTE and UNIX shell otracert/traceroute commands are enhanced in z/OS CS V1R4 to support IPv6 IP addresses.

See “Traceroute enhancements” on page 76 for updates to Traceroute in z/OS CS V1R4 that are not related to IPv6 support.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Migration procedures

If you want to take advantage of the IPv6 support for Traceroute, perform the tasks in the following table.

Table 47. IPv6 support for Traceroute - Migration tasks

Task	Procedure	Reference
Exploit the Traceroute IPv6 support.	Specify IPv6 host names or IP addresses on the Traceroute command options.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

IPv6 support for IPv6 IPCS subcommands formatting

As a result of the new support for IPv6 addressing, some TCPIPICS subcommands are affected:

- The UDP parameter is removed from the TCPIPICS TREE subcommand and is added to the TCPIPICS HASH subcommand.
- A new parameter, ICMPV6, is added to the HASH subcommand.
- The following parameters are new for the TCPIPICS TREE subcommand:
 - ND (Neighbor Discovery)
 - ROUTEV4 (for IPv4 route information only)
 - ROUTEV6 (for IPv6 route information only)
- The ROUTE subcommand has the following new parameters:
 - All
 - IPV4
 - IPV6

See the tables in Chapter 3, “New and changed interfaces” on page 29 for information about the changes to statements and commands from release to release. Refer to *z/OS Communications Server: IP Diagnosis* for details on TCPIPICS subcommands.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

There are no migration procedures associated with the IPCS subcommand changes. The changes only affect dump analysis.

IPv6 support for event trace enhancements

In z/OS CS V1R4, the event trace functions are enhanced for IPv6 by allowing IPv6 addresses to be specified on the IPADDR trace option keyword to execute traces on IPv6 addresses. There are also IPv4 enhancements associated with event tracing; see “Event trace enhancements” on page 72 for details.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

If you want to take advantage of the IPv6 support for event trace enhancements, perform the tasks in the following table.

Table 48. IPv6 support for event trace enhancements - Migration tasks

Task	Procedure	Reference
Filter the TCPIP event trace by IPv6 addresses.	Code the IPv6 addresses (and optionally numeric IPv6 address prefixes) on the IPADDR keyword by specifying one of the following: <ul style="list-style-type: none"> The component trace SYS1.PARMLIB member CTIEZBxx The Trace CT command 	<i>z/OS Communications Server: IP Diagnosis</i>
Turn on the Neighbor Discovery (ND) trace option.	Add ND to the list of trace options to the component trace SYS1.PARMLIB member. This turns on the ND trace option at TCP/IP initialization. Issue a Trace CT command with "OPTIONS=(ND)" to turn on the ND trace option after TCP/IP initialization.	<i>z/OS Communications Server: IP Diagnosis</i>

IPv6 support for RAS packet trace and data trace

Packet trace and data trace functions are part of several RAS facilities that are enhanced for IPv6 in order to maintain, debug, and service z/OS CS in an IPv6 environment. Incoming and outgoing data can be traced on a z/OS host at the IP layer (packet trace) or the physical file system (PFS) layer (data trace). Captured traces (CTRACE component SYSTCPDA) can be further analyzed in a variety of new ways by using IPCS. Packet trace and data trace functions remain unchanged for IPv4 except for slight usability enhancements.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

There are no migration tasks associated with the IPv6 support for packet trace and data trace. The enhancements are automatically enabled.

IPv6 support for socket API commands

Some very basic IPv6 support (mapped addresses only) was added in CS for OS/390 V2R10. See "IPv6 API" on page 153 for information about the support provided in CS for OS/390 V2R10.

In z/OS CS V1R4, the following TCP/IP socket APIs are enhanced for IPv6:

- TCP/IP Call Instruction
- TCP/IP Macro
- TCP/IP REXX

See Table 24 on page 58 for a list of the TCP/IP socket APIs that are enabled for IPv6. Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for more detailed information about IPv6 support for TCP/IP socket API commands.

In z/OS CS V1R4, IPv6 basic and IPv6 advanced API support has been added to LE C/C++ and z/OS UNIX Assembler Callable Services API. Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for more detailed information about IPv6 basic and advanced application support. Refer to *z/OS C/C++ Run-Time Library Reference* for complete documentation of the z/OS

UNIX C sockets APIs and refer to *z/OS UNIX System Services Programming: Assembler Callable Services Reference* for information about z/OS UNIX Assembler Callable Services.

Restrictions

The following TCP/IP socket APIs are not supported for IPv6:

- Pascal API
- CICS sockets API
- TCP/IP C sockets API

What this change affects

- Application Development

Migration procedures

If you want to take advantage of the enhancements to the IPv6 TCP/IP socket API support, perform the task in the following table.

Table 49. IPv6 support for TCP/IP socket API commands - Migration task

Task	Procedure	Reference
Enable TCP/IP for IPv6 by tailoring your BPXPRMxx SYS1.PARMLIB member.	Add an AF_INET6 NETWORK statement to your BPXPRMxx member.	<i>z/OS Communications Server: IPv6 Network and Application Design Guide</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Chapter 5. z/OS V1R3 Communications Server release summary

z/OS CS did not ship new function for V1R3. For complete information on z/OS Communications Server, see the z/OS Internet Library Website:
<http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>.

Chapter 6. z/OS V1R2 Communications Server release summary

This chapter describes the major changes introduced in z/OS V1R2 Communications Server.

See Table 15 on page 23 for a complete list of the functional enhancements you should consider. See Chapter 3, “New and changed interfaces” on page 29 for information on new, changed, deleted, or obsolete statements, commands, and APIs.

For information about changes to File Transfer Protocol (FTP), see Chapter 9, “Migrating the FTP server and client” on page 167.

For information about changes to Telnet, see Chapter 10, “Migrating the Telnet server and client” on page 203.

For information about changes to Simple Network Management Protocol (SNMP), see Chapter 11, “Migrating the SNMP server and client” on page 231.

For information about changes to Domain Name Server (DNS), see Chapter 12, “Migrating to the BIND-based DNS name server” on page 249.

Migration considerations

As you migrate from a previous release to z/OS CS V1R2, consider the following:

- Support for the ASSORTEDPARMS and KEEPALIVEOPTIONS TCP/IP profile statements will be removed in a future release. If you currently use these profile statements, consider migrating to the newer profile statements that support the same parameters. All the parameters on ASSORTEDPARMS are also supported on the newer profile statements, IPCONFIG, TCPCONFIG, UDPCONFIG, and GLOBALCONFIG. The KEEPALIVEOPTIONS parameter is supported by TCPCONFIG. The behavior of the parameters on the new profile statements is different from ASSORTEDPARMS and KEEPALIVEOPTIONS. On the newer profile statements, a parameter value is only changed if the parameter is specified on the profile statement. On ASSORTEDPARMS and KEEPALIVEOPTIONS, a parameter value was reset to the default if the parameter was not specified.
- CS for OS/390 Kerberos is not supported in z/OS V1R2 Communications Server; if you were using CS for OS/390 Kerberos support, you must start using z/OS Security Server Kerberos. Refer to *z/OS Security Server Network Authentication Service Administration* and *z/OS Security Server Network Authentication Service Programming*.
- If you are using UNIX Telnet, FTP, or UNIX RSHD, you must add these Kerberos data sets:
 - EUVF.SEUVFLNK - add to the LNKLISTxx PARMLIB member
 - EUVF.SEUVFLPA - add to the LPALSTxx PARMLIB member
- SEZAMIG is no longer shipped. It is replaced by MIGLIB. Ensure that you include MIGLIB in your LINKLIST or STEPLIB.

The remainder of this chapter consists of sections that describe the general functions and enhancements new to z/OS V1R2 Communications Server, including any migration procedures. Be sure to also read the release summary sections in the

applications chapters of this document because they contain migration considerations for those applications (FTP, Telnet, SNMP, and Telnet).

Resolver enhancements

The resolver acts on behalf of application programs as a client that accesses name servers for name-to-address or address-to-name resolution. If a name server is not available, the resolver will use local definitions (such as `etc/hosts`, `HOSTS.SITEINFO` or `HOSTS.ADDRINFO`) to resolve the query for the requesting program. `TCPIP.DATA` statements control how (and if) the resolver uses name servers.

Prior to z/OS V1R2, the resolver function was implemented as part of the various socket APIs (Application Programming Interfaces) available on the z/OS platform. As a result, multiple versions of the resolver function were available, one for each type of socket API supporting resolver calls. All of these resolver libraries were quite similar in their support of resolver functions but had slight differences from an administrative and configuration perspective. For example, the resolver search logic to locate its configuration file (`TCPIP.DATA` file) varied depending on whether the application was using the TCP/IP provided Socket APIs or the C/C++ Socket API provided by the LE (Language Environment[®]) component of z/OS.

In z/OS V1R2, the various resolver libraries supported by the TCP/IP and LE APIs are now consolidated into a single resolver component. This allows consistent name resolution processing across all applications using the TCP/IP and LE socket APIs. The new consolidated resolver is automatically enabled on z/OS V1R2 and requires a new system address space that is automatically started during UNIX System Services initialization. The consolidated resolver offers several enhancements over previous releases:

- You can now specify `TCPIP.DATA` statements that will be used regardless of the application's environment or the socket API the application is using. This allows installations to specify `TCPIP.DATA` statements in single location for the entire operating system image and prevent end-users from being able to override these specifications. This support is provided by a new resolver setup statement, `GLOBALTCPIPDATA`.
- You can now specify the final search location of where `TCPIP.DATA` statements are found by using a new resolver setup statement, `DEFAULTTCPIPDATA`.

Notes:

1. The `TCPIP.DATA` statements can be contained in either an MVS data set or an HFS file.
2. z/OS V1R2 still supports a separate resolver for Simple Mail Transfer Protocol (SMTP). In addition, the new DNS BIND 9 has a resolver that is used by the DNS BIND 9 utilities (`nslookup`, `nsupdate`, and `dig`). Even though these TCP/IP applications have their own resolver facilities, they support the `GLOBALTCPIPDATA` and `DEFAULTTCPIPDATA` specifications.

For information about the DNS BIND 9 resolver, see Chapter 12, "Migrating to the BIND-based DNS name server" on page 249.

- Certain `TCPIP.DATA` statements can now be updated and placed in effect immediately without requiring applications to be stopped and restarted. This is performed by using the `MODIFY RESOLVER,REFRESH` command.
- Support is added for the `LOOKUP`, `SEARCH`, `SORTLIST` and `OPTIONS` directives by using new statements in the `TCPIP.DATA` statement. The `LOOKUP` directive specifies the order in which the Domain Name Server and/or local host tables should be used to satisfy name resolution requests. The `SEARCH`

| directive allows you to query host names that reside in various domains without
| having to specify a fully qualified domain name (FQDN). The SORTLIST directive
| allows you to specify a list of subnets and/or networks the resolver should prefer
| if it receives multiple addresses as the result of a gethostbyname. The OPTIONS
| directive allows the administrator to specify miscellaneous options, such as the
| number of dots that can appear in a host name before it is considered a fully
| qualified name and the ability to turn on an application resolver trace.

| Refer to *z/OS Communications Server: IP Configuration Reference* for the usage
| of TCPIP.DATA statements.

In order to improve the performance of resolver name server queries, consider configuring a local caching name server. The local name server will reduce the network traffic associated with resolver queries.

Restrictions

None.

What this change affects

- Customization
- Operations
- Performance

Migration procedures

Any installation currently using resolver support *requires* completing the *first task* in the following table. The remaining tasks are optional and if you do not perform them, the resolver will function as it did in previous releases.

Table 50. Resolver enhancements - Migration tasks

Task	Procedure	Reference
<p>Required; Define an OMVS segment for PASCAL applications that do not currently have an OMVS segment or a Default Segment defined. (This is required since the resolver will be using z/OS UNIX services to access Name Servers.) Also, any installations that make use of SNALINK LU6.2 or X.25 NCP Packet Switching Interface <i>must</i> define an OMVS segment for the user ID assigned to their started task procedure.</p> <p>Note: The resolver enforces the requirement, as documented in previous IP configuration documents, that the TCPIP.DATA MVS data set must have a format of fixed (F) or fixed block (FB). The resolver will support any fixed or fixed block data set; the logical record length (LRECL) must be between 80 and 256.</p>	<p>Understand that use of z/OS UNIX services requires a z/OS UNIX security context, referred to as an <i>OMVS segment</i>, for the user ID associated with any unit of work requesting these services. In other words, most user IDs requiring access to TCP/IP functions require an OMVS segment to be defined in Resource Access Control Facility (RACF).</p> <p>To satisfy the requirement for an OMVS segment in RACF, do one of the following:</p> <ul style="list-style-type: none"> • Identify all the users in your environment that use TCP/IP services and then define OMVS RACF segments for the associated user IDs. • Use the default OMVS segment support provided by RACF and z/OS UNIX for users and groups. <p>The default OMVS segments reside in the USER profile and GROUP profile. The names of these profiles are identified by the installation, using the BPX.DEFAULT.USER facility class profile. The application data field in the class profile contains the user ID, or the user ID/group ID, that is used to access the default OMVS segments for users and groups, respectively.</p>	<p><i>z/OS Communications Server: IP Configuration Guide</i></p>
<p>Optional; customize the new resolver.</p>	<p>Ensure your BPXPRMxx member has the new statement, RESOLVER_PROC, with the name you want to use. Update the provided sample resolver procedure, SEZAINST(RESOPROC), and setup file, SEZAINST(RESSETUP), with your changes.</p> <p>If you specify RESOLVER_PROC(NONE) in your BPXPRMxx member, you must start the resolver address space prior to starting TCPIP. TCPIP will not initialize unless the resolver is started.</p>	<p><i>z/OS UNIX System Services Planning, z/OS MVS Initialization and Tuning Reference, and z/OS Communications Server: IP Configuration Guide</i></p>
<p>Optional; use the new resolver.</p>	<p>Relink any application that uses the TCPIP Pascal or TCP/IP's C/C++ APIs to include the new resolver.</p> <p>Create or update TCPIP.DATA files to take advantage of new and changed statements.</p>	<p><i>z/OS Communications Server: IP Application Programming Interface Guide, z/OS Communications Server: IP Configuration Guide, and z/OS Communications Server: IP Configuration Reference</i></p>
<p>Optional; use the local DNS cache facilities.</p>	<p>Configure DNS caching-only name server.</p>	<p><i>z/OS Communications Server: IP Configuration Guide</i></p>
<p>Optional; change the location of the global and/or default TCPIP.DATA files.</p>	<p>Create new global and/or default TCPIP.DATA files and issue the MODIFY RESOLVER,REFRESH,SETUP= command, referencing the new TCPIP.DATA files.</p>	<p><i>z/OS Communications Server: IP Configuration Reference.</i></p>
<p>Optional; reread existing global and/or default TCPIP.DATA files.</p>	<p>Update existing global and/or default TCPIP.DATA files and issue the MODIFY RESOLVER,REFRESH command, referencing the new TCPIP.DATA files.</p>	<p><i>z/OS Communications Server: IP Configuration Reference</i></p>

Table 50. Resolver enhancements - Migration tasks (continued)

Task	Procedure	Reference
Optional; control the behavior of the resolver by using directives.	Specify the SEARCH, SORTLIST, and/or OPTIONS statements in TCPIP.DATA statements.	<i>z/OS Communications Server: IP Configuration Reference</i>
Optional; debug the resolver.	Start the resolver CTRACE (the resolver default trace SYS1.PARMLIB member is CTIRES00) and analyze the data.	<i>z/OS Communications Server: IP Diagnosis</i>
Optional; debug application resolver usage.	Use the TRACE RESOLVER debug facility with the SYSTCPT DD statement or RESOLVER_TRACE environment variable to collect the debug information.	<i>z/OS Communications Server: IP Diagnosis</i>

Intrusion Detection Services

Support for Traffic Regulation Management (TRM) was provided in CS for OS/390 V2R10 for regulation of TCP connections on a port basis (see “Traffic Regulation and Management (TRM)” on page 142). TRM is now part of Intrusion Detection Services. In z/OS V1R2 Communications Server, the TCP Traffic Regulation support allows management by application (for example, bound port and destination IP address). This allows different policies to be defined for each application, even though they may be bound to the same destination port. For example, TN3270 and otelnet can both use port 23. In CS for OS/390 V2R10, TRM managed port 23 as a single entity even though the characteristics of the TN3270 and otelnet applications are very different. In z/OS V1R2 Communications Server, TCP Traffic Regulation has the capability to manage these applications separately with policy unique to each application.

Additionally, the following new support is provided in z/OS V1R2 Communications Server:

Traffic regulation for UDP receive queues

UDP Traffic Regulation allows an installation to limit the number of packets (for non-PASCAL traffic) and the number of bytes that can be waiting on an application’s receive queue. This is accomplished by specifying one of four queue sizes in the UDP TR policy. Similar to TCP Traffic Regulation, three modes are supported:

- **Limit mode** discards the packet if the policy specifications are exceeded.
- **Simulated limit mode** notifies the installation that the policy specifications are exceeded but does not discard the packet.
- **Statistics gathering mode** gathers information about normal traffic patterns and can be used for determining initial policy definitions.

Attack detection, reporting, and prevention

Detected known attacks are already defused by the TCP/IP stack. However, the installation may not be aware that these possible attacks are occurring. This support allows an installation to be notified when these events occur if requested by policy. Additionally, policy can be used to define a restricted group of IP options and IP protocols. Policy can also be specified to turn on checks for suspicious fragmentation, suspicious outbound RAW packets, and potential perpetual echoes.

Scan detection and reporting

Scans are recognized as the result of multiple information gathering events from a single source IP address within a defined period of time. Scanning in and of itself is not harmful. However, many serious attacks are preceded by

information-gathering scans. Because scans by their nature must use reliable source IP addresses, they can be interesting events to monitor. The individual packets used in a scan can be categorized as normal, possibly suspicious, or very suspicious. To control the performance impact and analysis load of scan monitoring, scan policy will allow an installation to specify which category of traffic should be monitored as potential scan events. Policy also specifies the number of events (threshold) and the interval of time that define a scan event. Fast Scan and Slow Scan threshold and intervals can be defined.

Tracing and reporting

In CS for OS/390 V2R10, notification of a policy exception was reported to syslogd. z/OS V1R2 Communications Server also provides the options to send a notification to the MVS console and to trace the packet to a IDS-specific CTRACE component, SYSTCPIS. The trace options can specify tracing of headers only, a partial packet, or the full packet. The SYSTCPIS CTRACE can be accessed using the same tools used to format a TCP packet trace. The data space used for the SYSTCPIS CTRACE is set up using options specified in the CTIIDSxx parmlib member.

In addition, z/OS V1R2 Communications Server enhances statistics reporting so that it can be limited to reporting only intervals in which exceptions occurred. This is accomplished by requesting EXCEPTSTATS rather than STATISTICS.

Furthermore, in z/OS V1R2 Communications Server the trmdstat utility is extended to provide summary reports for UDP traffic regulation, attacks, and scan events. Trmdstat now also provides a statistics report for displaying the statistics data collected when policy requests STATISTICS or EXCEPTSTATS for traffic regulation or attack detection.

Most of the syslogd messages issued by trmd were modified in z/OS V1R2 Communications Server. Some messages were deleted and others were added. Refer to *z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)* for complete information on the messages associated with the Intrusion Detection Services function.

A high level display of overall IDS activity will be available through the Netstat IDS/-k command. IBM recommends that your installation restricts access to this command in the z/OS UNIX and TSO environments with the new security resource: EZB.NETSTAT.mvsname.tcpprocname.IDS. For example,

```
RDEFINE SERVAUTH EZB.NETSTAT.mvsname.tcpprocname.IDS UACC(NONE)

PERMIT EZB.NETSTAT.mvsname.tcpprocname.IDS CLASS(SERVAUTH)
      ID(userid) ACCESS(READ)
```

Restrictions

Policy for the new z/OS CS V1R2 IDS functions must be defined in the LDAP server. It cannot be defined in the Policy Agent configuration file.

Dependencies

Policy is provided by the Policy Agent (Pagent). Syslogd and trmd must be active in order to obtain statistics and log records written to syslogd.

Incompatibilities

The TCP Traffic Management policy in CS for OS/390 V2R10 was defined as part of the QoS policy with a PolicyScope of TR. It could only be defined in the Policy Agent configuration file; the LDAP server was not supported.

The new z/OS V1R2 Communications Server IDS policy will only be available in LDAP. TCP TR policy will also be supported in LDAP as part of the IDS policy. For upward compatibility, TR policy that existed in CS for OS/390 V2R10 will continue to be supported in the Policy Agent configuration file and will work unchanged, with the exception that it will be displayed differently by the pasearch command (as an IDS policy instead of a QoS policy with policy scope TR). Also, a TR policy will not be displayed by the Netstat SLAP/-j command. However, if you want to use any of the new intrusion detection/traffic regulation support, be aware that the new functions are only available through LDAP policy. You can use a combination of the LDAP policy for the new functions and then keep the TCP traffic regulation policy in the configuration file, although this is not recommended.

What this change affects

- Customization
- Security

Migration procedures

Existing TR policy defined in the Policy Agent configuration file will continue to work as it did in CS for OS/390 V2R10. If you want to take advantage of the Intrusion Detection Services function, perform the tasks in the following table.

Table 51. Intrusion Detection Services - Migration tasks

Task	Procedure	Reference
Plan which intrusion types to monitor and how to respond.	Evaluate your normal traffic to ensure that any new policy will continue to allow legitimate requests. This is particularly important if your policy could cause packets that would otherwise be processed to be dropped when LIMIT mode is specified. Traffic Regulation and certain attack types fall into this category. To help determine TR policy, consider running with the statistics action first (ibm-idsTypeActions:STATISTICS) to determine policy values. Next, for TR and attack detection policies, run with the LOG but not the LIMIT action (ibm-idsTypeActions:LOG ibm-idsNotification:SYSLOG) to test out the policy limits. Ensure the trmd daemon and syslogd are started when running the above. TRMD handles recording statistics and log data to syslogd.	<i>z/OS Communications Server: IP Configuration Guide and z/OS Communications Server: IP Configuration Reference</i>
Define IDS policies and actions.	Define Intrusion detection policy in LDAP for the events to be detected or monitored. For Traffic Regulation and Attacks, once the installation has determined a policy that allows legitimate traffic, move to limit mode with logging (ibm-idsTypeActions:LOG ibm-idsTypeActions:LIMIT ibm-idsNotification:SYSLOG). 'Limit' will drop packets based on the policy specifications. 'Log' provides notification of the actions taken.	<i>z/OS Communications Server: IP Configuration Guide and z/OS Communications Server: IP Configuration Reference</i>

Table 51. Intrusion Detection Services - Migration tasks (continued)

Task	Procedure	Reference
Update TCP profile.	If requesting scan detection, consider defining ports that are not used as RESERVED on the PORT or PORTRANGE statement in the TCP profile. For example: PORT 19 TCP RESERVED	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Activate intrusion detection.	Start Policy Agent and TRMD. Syslogd must also be started if logging or statistics are requested.	<i>z/OS Communications Server: IP Configuration Reference</i>

Sysplex Distributor policy enhancements

This function is an enhancement to the CS for OS/390 V2R10 Policy Agent function (see “Policy Agent enhancements” on page 139) and CS for OS/390 V2R10 Sysplex Distributor function (see “Sysplex Distributor” on page 135). In CS for OS/390 V2R10, the Sysplex Distributor was enhanced to select a target stack depending on the QoS fraction and WLM weight. In z/OS V1R2 Communications Server, the Sysplex Distributor is further enhanced to calculate additional QoS fractions per-service level, thus allowing the Sysplex Distributor to provide a more efficient and fair distribution of connections.

Incompatibilities

The following incompatibilities apply:

- The new QoS policy action changes will not be used if a CS for OS/390 V2R10 Sysplex Distributor is used, or if a z/OS V1R2 Communications Server Sysplex Distributor has only CS for OS/390 V2R10 sysplex targets.
- The new z/OS V1R2 Communications Server QoS policy action functions will be active only if policy actions with outbound interfaces (of the targets) are configured on the Sysplex Distributor and corresponding policy actions with the same service level names are configured on the targets.

What this change affects

- Operations
- Performance
- Usability

Migration procedures

If you want to take advantage of the Sysplex Distributor policy enhancements, perform the tasks in the following table.

Table 52. Sysplex Distributor policy enhancements - Migration tasks

Task	Procedure	Reference
Verify that there is a common Policy Agent listening port on all targets and distributors and that the port is unused by any application in the sysplex.	Check in /etc/services to see the Policy Agent listening port - pagentQosListener, and the Policy Agent sending port - pagentQosCollector. If any application is using one of the ports, then change this directory to specify a new port number. The same port number must be specified on all targets and distributors in the Sysplex.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Verify that there is a common Policy Agent sending port on all targets and distributors that is unused by any application in the sysplex.	The /etc/services install file contains the suggested Policy Agent listening and sending ports.	

Table 52. Sysplex Distributor policy enhancements - Migration tasks (continued)

Task	Procedure	Reference
Verify that the above ports are specified in the TCPIP PROFILE.	Ensure that the PROFILE.TCPIP contains the assignments for the above ports.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Complete the sysplex definitions and verify that dynamic XCF addresses are being used.	Ensure that DYNAMICXCF is configured on IPCONFIG statement. The PAGENT TCP connections use the XCF IP addresses.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Ensure that the Policy Agent performance monitor function is active on the target stacks and the distributing stacks.	Ensure that the PolicyPerfMonitorForSDR statement has an enabled flag.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Ensure that a policy action with the same service level name is defined on each of the appropriate target stacks and also on the distributing stack for these targets.	<p>For each service level that should have z/OS V1R2 Communications Server load distribution active, verify that policy actions on the appropriate targets and distributors have the same name; the names for each service level should be unique across the sysplex.</p> <p>Ensure that the policy action on the distributor has the outbound interfaces of the target's DXCFs. The policy action on the distributor and targets should be policy scope DataTraffic or Both.</p> <p>Ensure that any service level that should <i>not</i> have the new z/OS V1R2 Communications Server load distribution function is not defined on the distributor. Use the CS for OS/390 V2R10 load distribution instead.</p>	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Ensure that the rules that will be used by the distributor are identified to improve performance during the target statistics gathering operation.	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Run with an LDAP server using the schema version 3. Create an ibm-policyGroup object for sysplex rules and code the new auxiliary class, ibm-policyGroupLoadDistributionAuxClass. Code the new attribute, ibm-policyGroupForLoadDistribution TRUE, on this new object. • Do not run with an LDAP server. Code ForLoadDistribution TRUE on the PolicyRule statement if this is a sysplex rule. 	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Ensure that any backup distributing stack has the same policy action configuration definitions as the active distributing stack for the corresponding VIPA targets that it is backing up. It will also need to have the Policy Agent performance monitor function active.	Verify that the maximum QoS connections on the above policy action at each target that map to a port (application) do not exceed the target's policy action TR total connections for that port (application).	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Coordinate Policy Action TCP connection limits on each target with overall TRMD connection limits on each target.	Verify that the maximum QoS connections on the above policy action at each target that map to a port (application) do not exceed the target's policy action TR total connections for that port (application).	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Table 52. Sysplex Distributor policy enhancements - Migration tasks (continued)

Task	Procedure	Reference
Ensure that any backup distributing stack has the same policy action configuration definitions as the active distributing stack for the corresponding VIPA targets that it is backing up. It will also need to have the Policy Agent performance monitor function active.	The same PolicyActions defined above on the active distributing stack should be defined on the backup. PolicyPerfMonitorForSDR statement must have an enabled flag.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Ensure that PAGENT is running on the distributor and all of its target nodes.	Start PAGENT from the z/OS shell or as a started task on each MVS system that is part of the sysplex.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Policy Agent enhancements

The OS/390 UNIX Policy Agent was introduced in CS for OS/390 V2R7. In CS for OS/390 V2R10, it was enhanced with new function, including version 2 schema (see “Policy Agent enhancements” on page 139). The policy schema supported by the Policy Agent for defining policy objects on an LDAP server is enhanced in z/OS V1R2 Communications Server to better match the current RFC draft. The z/OS V1R2 Communications Server schema enhancements include:

- Improved LDAP retrieval performance
- Tighter integration between policy objects
- The ability to identify any LDAP object as belonging to the generic policy class
- Better search filtering, and the ability to differentiate between rule-specific and reusable policy conditions and actions
- Support for the MODIFY commands to immediately refresh policies, and to change or query the Policy Agent log level, trace level, or debug level

Restrictions

None.

What this change affects

- Customization
- Diagnosis
- Performance
- Usability

Migration procedures

If you want to take advantage of the Policy Agent enhancements, perform the tasks in the following table.

Table 53. Policy Agent enhancements - Migration tasks

Task	Procedure	Reference
Run the Policy Agent as a background shell process.	When starting Policy Agent from a shell session, run it in the background by specifying a trailing ampersand (&) character on the command line.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Table 53. Policy Agent enhancements - Migration tasks (continued)

Task	Procedure	Reference
<p>Determine if you want to allow non-superuser users to issue the pasearch command. If you do, then define appropriate security product authorization for policies. If you do not, then define security product authorization so that only superusers can use the pasearch command.</p>	<p>Define security product profiles in the SERVAUTH class using the following prototype: EZB.PAGENT.<sysname>.<TcplImage>.<ptype></p>	<p><i>z/OS Communications Server: IP Configuration Guide</i></p>
<p>Install the proper set of schema definitions on an LDAPv2 or LDAPv3 server.</p>	<p>Install the files pagent_at.conf and pagent_oc.conf (available in the /usr/lpp/tcpip/samples directory) in the initial configuration file of an LDAP protocol version 2 server. Modify the cn=schema subschema entry using ldapmodify commands on an LDAP protocol version 3 server. The set of files to use (available in the /usr/lpp/tcpip/samples directory) depend on the schema definitions already in place on the LDAP server.</p>	<p>Read the section on installing the schema definitions in <i>z/OS Communications Server: IP Configuration Guide</i></p>
<p>Determine if policy conditions and actions in existing rules should be rule-specific or reusable objects.</p>	<p>Analyze existing policy conditions and actions. Any conditions or actions that are specific to a single rule can be attached to the condition association or action association objects associated with the policy rule (see next task). All conditions and actions that are (or may be) reusable among several rules should become reusable objects. These should be specified using the new ibm-policyConditionInstance and ibm-policyActionInstance object classes, and placed in the directory tree anchored under an instance of the ibm-policyRepository object class.</p>	<p><i>z/OS Communications Server: IP Configuration Guide</i></p>
<p>Migrate schema version 2 conditions and actions to schema version 3.</p>	<p>Copy the information on the ibm-policyRuleConditionList and ibm-policyRuleActionList attributes to the new ibm-policyRuleConditionAssociation and ibm-policyRuleActionAssociation object classes. Either change the ibm-policyRuleConditionList and ibm-policyRuleActionList attributes to the ibm-policyRuleConditionListDN and ibm-policyRuleActionListDN attributes, or omit them if the new association object classes are under the policy rule in the directory tree structure. Change the ibm-policyCondition object class to ibm-policyConditionAuxClass, ibm-policyAction object class to ibm-policyActionAuxClass, and ibm-policyTimePeriodCondition object class to ibm-policyTimePeriodConditionAuxClass. Also change the ibm-networkingPolicyCondition object class to ibm-networkingPolicyConditionAuxClass, and ibm-serviceCategories object class to ibm-serviceCategoriesAuxClass.</p>	<p><i>z/OS Communications Server: IP Configuration Guide</i></p>
<p>Specify days of the month in reverse order in time period conditions.</p>	<p>Change the ibm-ptpConditionDayOfMonthMask attribute from 31 bits to 62 bits.</p>	<p><i>z/OS Communications Server: IP Configuration Guide</i></p>

Table 53. Policy Agent enhancements - Migration tasks (continued)

Task	Procedure	Reference
Specify correct object classes in policy group objects.	If any policies being migrated from schema version 2 to schema version 3 have any <code>ibm-policyGroup</code> objects defined, only specify the <code>ibm-policyGroupLoadDistributionAuxClass</code> , the <code>ibm-policyGroupContainmentAuxClass</code> , and/or <code>ibm-policyRuleContainmentAuxClass</code> objectClass values if the policy group objects will <i>only</i> be processed by z/OS V1R2 Communications Server systems. If these objects will be processed by a Policy Agent on a release prior to z/OS V1R2 Communications Server, then do not specify these objectClass values.	<i>z/OS Communications Server: IP Configuration Guide</i>
Use policy subtree pointers to enhance performance of LDAP object retrieval.	If your directory tree is structured such that large numbers of objects are not contained in the subtree identified with the <code>SearchBasedDN</code> parameter on the <code>ReadFromDirectory</code> statement, add the <code>ibm-policySubtreesPtrAuxClass</code> object class, and <code>ibm-policySubtreesAuxContainedSet</code> attributes to any objects in the initial set of objects retrieved, to retrieve additional subtrees of objects during the initial search. This avoids having those objects individually retrieved later.	<i>z/OS Communications Server: IP Configuration Guide</i>
Use policy keywords to allow object filtering.	Add the <code>ibm-policyKeywords</code> attribute to any policy object to allow that object to be filtered using keywords specified using the <code>SearchPolicyKeyword</code> parameter on the <code>ReadFromDirectory</code> statement.	<i>z/OS Communications Server: IP Configuration Guide</i>
Enable proper retrieval of the LDAP policy objects.	Configure the <code>LDAP_SchemaVersion</code> , <code>LDAP_AbstractPolicy</code> , and <code>SearchPolicyKeyword</code> attributes on the <code>ReadFromDirectory</code> configuration statement, if necessary, in order to retrieve the correct set of objects from the LDAP server.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Change policy automation.	If any automation has been performed for the <code>pasearch</code> command output, make appropriate changes for the minor differences in the command output.	<i>z/OS Communications Server: IP System Administrator's Commands.</i>

OROUTED to OMPROUTE migration

OROUTED was introduced in CS for OS/390 V2R4 and the OMPROUTE routing daemon was introduced in CS for OS/390 V2R6. OROUTED supports RIP1 and RIP2 protocols. OMPROUTE also supports RIP1 and RIP2, as well as Open Shortest Path First (OSPF) protocols. In z/OS V1R2 Communications Server, you are encouraged to use OMPROUTE instead of OROUTED because in a future release, support for OROUTED will be dropped (it is not needed since OMPROUTE also supports RIP protocols).

z/OS V1R2 Communications Server adds a function to OROUTED (invoked with the `-c` parameter) to make migration to OMPROUTE easier. With the `-c` parameter, OROUTED takes the routes, interfaces, and filters that currently exist and creates a file that may be used as an OMPROUTE profile. Even though some manual changes to the OMPROUTE profile may be required, this function saves time and effort by having OROUTED perform the configuration conversion. With `-c` as a start

parameter, OROUTED does not modify the IP route table and does not send or receive RIP messages nor process RIP information.

Note: You should review the results of using OROUTED -c to ensure that the simplest configuration is produced. It is possible that a complex OROUTED configuration becomes a very complex OMPROUTE configuration when a much simpler configuration would work. Furthermore, your existing OROUTED configuration must be coded correctly. OROUTED -c does a direct migration of existing interfaces and routes and does not correct pre-existing configuration or environment errors. Likewise, OROUTED does not perform network design.

For more information on the configuration and functional differences between OROUTED and OMPROUTE, refer to *z/OS Communications Server: IP Configuration Reference*.

Restrictions

None.

What this change affects

- Customization
- Usability

Migration procedures

If you want to take advantage of the OROUTED to OMPROUTE migration function, perform the task in the following table.

Table 54. OROUTED to OMPROUTE migration - Migration Task

Task	Procedure	Reference
Migrate from OROUTED to OMPROUTE.	<ol style="list-style-type: none"> 1. Start or MODIFY OROUTED with -c parameter. (If started with -c , OROUTED will terminate when the process is complete.) 2. Take the conversion file and put it in the appropriate directory or data set for OMPROUTE. 3. Follow the steps in <i>z/OS Communications Server: IP Configuration Guide</i> on configuring OMPROUTE. You will need to review and update the new OMPROUTE configuration file and the TCP/IP profile. For example, for point to point interfaces that do not support sending to a broadcast address, a nonzero destination address must be specified on the RIP interface statement if RIP version 1 is to be sent over the interface. A second example: for passive entries in the gateways file for OROUTED, the conversion file provides suggested BEGINROUTES statements for the TCPIP profile. 4. Stop OROUTED if the daemon is active. 5. Start OMPROUTE using the conversion file as the configuration file. 	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

OMPROUTE to allow RIP1 and RIP2 packets over the same interface

z/OS V1R2 Communications Server allows OMPROUTE to receive RIP1 and RIP2 packets over the same RIP interface. This eases migration in scenarios where networks are being migrated between RIP1 and RIP2 and it allows OMPROUTE to operate with routers that provide different levels of RIP updates.

Restrictions

The following restrictions apply:

- This enhancement only affects RIP packets received, not ones sent.
- OMPROUTE can only send one version of an RIP packet over a given interface. Therefore, if an RIP interface receives an RIP request of a version other than the one that it can send, the request will be ignored.
- If RECEIVE_RIP is coded to ANY, unauthenticated RIPV1 packets will be accepted, even if RIPV2 authentication parameters are coded for the interface.

What this change affects

- Customization
- Usability
- Availability
- Operations

Migration procedures

If you want to take advantage of the OMPROUTE to allow RIP1 and RIP2 packets over the same interface function, perform the tasks in the following table.

Table 55. OMPROUTE to allow RIP1 and RIP2 packets over the same interface - Migration tasks

Task	Procedure	Reference
Control the versions of RIP updates that will be accepted over an interface.	Code the RECEIVE_RIP parameter on the RIP_INTERFACE configuration statement.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Ensure that non-authenticated updates are not accepted over an RIP interface.	Code the following: <ul style="list-style-type: none">• AUTHENTICATION_KEY parameter on RIP_INTERFACE configuration statement• RIPV2=YES on the RIP_INTERFACE configuration statement• RECEIVE_RIP=RIP2 on the RIP_INTERFACE configuration statement. (This is necessary because the RIP Version 2 RFC requires interfaces that accept RIP1 packets to accept them unconditionally even if authentication is required and even though RIP1 does not support authentication.)	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Replaceable static routes

Static routes can be defined as replaceable in BEGINROUTES blocks. In z/OS V1R2 Communications Server, OMPROUTE can replace these routes with dynamic routes. In previous releases, static routes could not be replaced by dynamic routes.

If a static route is not defined as replaceable, it will behave as it did in previous releases and will override all other routes.

Restrictions

The following restrictions apply:

- Only OMPROUTE's treatment of static routes is updated. Stack or OROUTED usage is not changed.

- Only BEGINROUTES supports definition of replaceable static routes. GATEWAY statements are not changed.
- Replaceable and non-replaceable static routes cannot coexist to the same destination.
- Replaceable static routes cannot be defined to any destination that corresponds to a dynamic VIPA for which the TCP/IP stack is a sysplex distributor target.

What this change affects

- Customization
- Diagnosis
- Availability
- Performance
- Security

Migration procedures

If you want to take advantage of the replaceable static routes function, perform the second task in the following table. If you want to continue with pre-V1R2 behavior, perform the first task.

Table 56. Replaceable static routes - Migration tasks

Task	Procedure	Reference
Force OMPROUTE to always use a static route regardless of availability of better dynamic routes (pre-z/OS V1R2 behavior).	Do one of the following: <ul style="list-style-type: none"> • Do <i>not</i> define a static route as REPLACEABLE in the BEGINROUTES statement. • Define the route as NOREPLACEABLE. • Define the static route with a GATEWAY statement. 	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Allow OMPROUTE to replace a static route if a dynamic route becomes available.	Code the following: <ul style="list-style-type: none"> • Code the REPLACEABLE option to define a static route as replaceable in the BEGINROUTES statement. • If you are currently using a GATEWAY statement to define the static route, you will need to convert to BEGINROUTES to exploit the REPLACEABLE parameter. 	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

OMPROUTE wildcard IP addressing enhancement

For OMPROUTE, wildcard IP address processing has been enhanced. If the TCP/IP stack does not provide an interface address and name for OMPROUTE that is in the OMPROUTE profile, then the next most specific wildcard address will be used.

Restrictions

None.

What this change affects

- Customization
- Usability

Migration procedures

There are no migration procedures for the OMPROUTE wildcard IP addressing enhancement.

Additional RIP filter for OMPROUTE

In z/OS V1R2 Communications Server, OMPROUTE introduces a new RIP input filter that allows you to ignore RIP routing table broadcasts from a particular gateway.

Restrictions

None.

What this change affects

- Customization
- Usability
- Operations

Migration procedures

If you want to take advantage of the additional RIP filter for OMPROUTE function, perform the task in the following table.

Table 57. Additional RIP filter for OMPROUTE- Migration task

Task	Procedure	Reference
Ignore RIP routing table broadcasts from a particular gateway.	Code the IGNORE_RIP_NEIGHBOR statement indicating the IP address of the gateway to be ignored.	<i>z/OS Communications Server: IP Configuration Reference</i>

OSPF MD5 authentication

The OMPROUTE routing daemon implements Open Shortest Path First (OSPF) and RIP. In z/OS V1R2 Communications Server, OMPROUTE can participate in router networks implementing Message Digest (MD5) cryptographic authentication, which is superior to the simple password method previously available. In addition, in z/OS V1R2 Communications Server you can define authentication type by interface, instead of only by area as in previous releases. This allows greater flexibility in configuring authentication and eliminates the need to consider authentication types when defining OSPF areas.

For information about MD5 authentication, refer to Appendix D of RFC 2328. Previous versions of OMPROUTE implement authentication as described in Appendix D of RFC 1583.

Restrictions

The following restrictions apply:

- Only a single MD5 key per interface is supported. Multiple keys based on time of day or other considerations are not supported.
- All OSPF routers on a network must be implementing the same authentication scheme with the same key.

What this change affects

- Security
- Availability

Migration procedures

If you want to take advantage of the OSPF MD5 authentication function, perform the tasks in the following table. If you want to continue using password authentication on an area basis as supported in CS for OS/390 V2R10 or earlier, no action is required.

Table 58. OSPF MD5 authentication - Migration tasks

Task	Procedure	Reference
Vary authentication type by interface.	Code the new AUTHENTICATION_TYPE keyword on the OSPF_INTERFACE statement. For compatibility with previous releases, this statement defaults to the value coded on the area on which the interface attaches.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Specify authentication type of a virtual link.	Code the new AUTHENTICATION_TYPE keyword on the VIRTUAL_LINK statement. For compatibility with previous releases, this statement defaults to the value coded for the backbone area.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Make MD5 authentication the default type for an area.	Code the new value MD5 for the AUTHENTICATION_TYPE keyword on the AREA configuration statement.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Use MD5 authentication over a network.	<ul style="list-style-type: none"> • Code AUTHENTICATION_TYPE=MD5 on all OSPF interfaces attached to the network if the default authentication scheme for the area is not MD5. • Code the same 16-byte MD5 key as the AUTHENTICATION_KEY value on all OSPF interfaces attached to the network. 	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Use MD5 authentication over a virtual link.	<ul style="list-style-type: none"> • Code AUTHENTICATION_TYPE=MD5 on the VIRTUAL_LINK statements on both sides of the link if the default authentication scheme for the backbone area is not MD5. • Code the same 16-byte MD5 key as the AUTHENTICATON_KEY value on both sides of the link. 	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Verify the authentication type used on an interface.	Display the interface: D TCPIP, stackname, OMP, INTERFACE,NAME=name. Authentication type used over that interface will be provided in the display	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Create an MD5 key from an existing password.	Use the pwtokkey command.	<i>z/OS Communications Server: IP Configuration Reference</i>

Native Socket API TCP_NODELAY support

z/OS V1R2 Communications Server provides support to allow the Nagle algorithm (RFC 896) to be toggled on and off at the socket layer. Turning off the Nagle algorithm can result in better response time for some interactive applications. z/OS V1R2 Communications Server includes support for TCP_NODELAY on the setsockopt and getsockopt API calls for the following APIs:

- TCP/IP C-sockets (non-UNIX sockets)
- Sockets Extended assembler macro API
- Sockets Extended Call API
- CICS sockets (both call and C)

Restrictions

None.

What this change affects

- Performance
- Application Development

Migration procedures

If you want to take advantage of the Native Socket API TCP_NODELAY support function, perform the appropriate tasks in the following table.

Table 59. Native Socket API TCP_NODELAY support - Migration tasks

Task	Procedure	Reference
Toggle the use of the Nagle algorithm if running an application using one of the following APIs: <ul style="list-style-type: none">• Sockets Extended assembler macro API• Sockets Extended Call API• CICS sockets extended API	Specify TCP_NODELAY as the option name on the setsockopt() API call.	<i>z/OS Communications Server: IP Application Programming Interface Guide</i> and <i>z/OS Communications Server: IP CICS Sockets Guide</i>
Toggle the use of the Nagle algorithm if running an application using one of the following APIs: <ul style="list-style-type: none">• TCP/IP C-sockets API (non-UNIX sockets)• CICS C-sockets API	Specify IPPROTO_TCP as the level and TCP_NODELAY as the option name on the setsockopt() API call.	<i>z/OS Communications Server: IP Application Programming Interface Guide</i> and <i>z/OS Communications Server: IP CICS Sockets Guide</i>
Query if the Nagle algorithm is being used for a socket if running an application using one of the following APIs: <ul style="list-style-type: none">• Sockets Extended assembler macro API• Sockets Extended Call API• CICS sockets extended API	Specify TCP_NODELAY as the option name of the getsockopt() API call.	<i>z/OS Communications Server: IP Application Programming Interface Guide</i> and <i>z/OS Communications Server: IP CICS Sockets Guide</i>
Query if the Nagle algorithm is being used for a socket if running an application using one of the following APIs: <ul style="list-style-type: none">• TCP/IP C-sockets API (non-UNIX sockets)• CICS C-sockets API	Specify IPPROTO_TCP as the level and TCP_NODELAY as the option name on the getsockopt() API call.	<i>z/OS Communications Server: IP Application Programming Interface Guide</i> and <i>z/OS Communications Server: IP CICS Sockets Guide</i>

Netstat enhancements

z/OS V1R2 Communications Server includes enhancements to the netstat commands, as follows:

- Netstat filter enhancements
- Netstat performance counters
- Restrict access to netstat commands

All three of these areas of enhancement are discussed in this section.

Netstat filter enhancements

z/OS V1R2 Communications Server includes enhancements to the netstat commands to allow a choice to include or exclude the TN3270 Server Connections from the netstat ALL/-A, ALLCONN/-a, CONN/-c, BYTEINFO/-b, CLIENTS/-e, and SOCKETS/-s reports. The following netstat entries include new and changed filter options:

- TSO NETSTAT command: ALL, ALLCONN, BYTEINFO, CLIENTS, CONN, and SOCKETS options
- UNIX onetstat/netstat command: -A, -a, -b, -c, e, and -s options
- MVS D TCPIP,NETSTAT command: ALLCONN, BYTEINFO, CONN, and SOCKETS options

In addition, the existing filter support for CLIENT/-E, IPADDR/-I, and PORT/-P is enhanced to work for netstat SOCKETS/-s so that the netstat SOCKETS/-s report can provide the response on the specified client name, IP address, or port number. The existing filter support for IPADDR/-I, and PORT/-P is enhanced to work for netstat ALL/-A so that the netstat ALL/-A report can provide the response on the specified IP address, or port number.

See the netstat entries in Table 20 on page 36, Table 21 on page 43, and Table 22 on page 49 for more information on the new and changed filter options. Refer to *z/OS Communications Server: IP Configuration Reference* for complete information on operator commands. Refer to *z/OS Communications Server: IP System Administrator's Commands* for complete information on TSO and UNIX commands.

Restrictions

None.

What this change affects

- Customization
- Performance

Migration procedures

There are no migration procedures for the netstat filter enhancements unless you want to use the new and changed options. If so, see the netstat entries in Table 20 on page 36, Table 21 on page 43, and Table 22 on page 49.

Netstat performance counters

z/OS V1R2 Communications Server enhances the netstat commands to show performance characteristics and identify performance problems. The following netstat entries include new or changed performance options:

- TSO NETSTAT command: ALL, DEVLINKS, HELP, and STATS options
- UNIX onetstat/netstat command: -A, -d, -S, and -? options

- MVS D TCPIP,,NETSTAT command: STATS option; and MVS D TCPIP,,HELP command: STATS option

See the netstat entries in Table 20 on page 36, Table 21 on page 43, and Table 22 on page 49 for more information on the new and changed performance options. Refer to *z/OS Communications Server: IP Configuration Reference* for complete information on operator commands. Refer to *z/OS Communications Server: IP System Administrator's Commands* for complete information on TSO and UNIX commands.

Restrictions

None.

What this change affects

- Customization
- Performance

Migration procedures

There are no migration procedures for the netstat performance counters unless you want to use the new and changed options. If so, see the netstat entries in Table 20 on page 36, Table 21 on page 43, and Table 22 on page 49.

Restrict access to netstat commands

z/OS V1R2 Communications Server provides a new way to control access to the netstat command at both the overall command level and command option level. You can permit or disallow user access to specific netstat options or resources.

Restrictions

This function only applies to TSO and UNIX shell netstat command users.

What this change affects

- Customization
- Installation
- Operations
- Security

Migration procedures

If you want to take advantage of the restrict access to netstat command function, perform the task in the following table.

Table 60. Restrict access to netstat command function - Migration task

Task	Procedure	Reference
Use access control to netstat command and its options from the TSO and UNIX shell.	Define the security product resource name, EZB.NETSTAT.mvsname.tcprocname.option, in the SERVAUTH class. Ensure that the SERVAUTH class is active and RACLISTed. Permit users READ access to the resource name.	<i>z/OS Communications Server: IP System Administrator's Commands</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

z/OS UNIX RSHD Kerberos support

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications using secret-key cryptography. The Kerberos support provided in z/OS V1R2 Communications Server provides greater security for certain applications and allows the use of these applications to secure data traffic in the network. Specifically, z/OS V1R2 Communications Server introduces Kerberos support for authentication for the following applications:

- The UNIX remote shell execution (rsh) server — authentication support provided by the Kerberos 5 protocol and the GSSAPI protocol
- The FTP client and FTP server — authentication support provided by the GSSAPI protocol
- The UNIX Telnet server — authentication support provided by the Kerberos 5 protocol

If you are using UNIX Telnet, FTP, or UNIX RSHD, you must add these Kerberos data sets:

- EUVF.SEUVFLNK - add to the LNKLSTxx PARMLIB member
- EUVF.SEUVFLPA - add to the LPALSTxx PARMLIB member

The Kerberos support for the UNIX RSHD server is described in this section. See “Kerberos support for the FTP server and client” on page 185 for the FTP client and FTP server considerations. See “z/OS UNIX Telnet (otelnetd) server – Kerberos support” on page 216 for the UNIX Telnet server considerations.

Restrictions

None.

Incompatibilities

The zSeries Key Distribution Center (KDC) is incompatible with Windows® 2000 Kerberos applications. Windows 2000 applications must use the Windows KDC. To support Windows 2000 applications, a cross-realm connection between the zSeries KDC and the Windows KDC is required.

What this change affects

- Security
- Customization
- Operations

Migration procedures

If you want to take advantage of the Kerberos support function for the UNIX RSHD server, perform the tasks in the following table. See “Kerberos support for the FTP server and client” on page 185 for the FTP client and FTP server considerations. See “z/OS UNIX Telnet (otelnetd) server – Kerberos support” on page 216 for the UNIX Telnet server considerations.

Table 61. Kerberos support for the UNIX RSHD server - Migration tasks

Task	Procedure	Reference
Enable authentication in the RSH server.	Specify the -k parameter when invoking the RSH server.	<i>z/OS Communications Server: IP Configuration Reference</i>

Table 61. Kerberos support for the UNIX RSHD server - Migration tasks (continued)

Task	Procedure	Reference
Require encryption in the RSH server.	Specify the -e parameter when invoking the RSH server.	<i>z/OS Communications Server: IP Configuration Reference</i>

Application-driven policy classification

In z/OS V1R2 Communications Server, users can assign multiple QoS service levels (based on the content of data being delivered from a given server) for outgoing traffic that an application generates. For example, a user can assign specific QoS service levels to selected URLs that the IBM HTTP server for z/OS processes. This allows users to prioritize the outgoing traffic for the HTTP server based on the business priorities associated with different URLs.

The z/OS Language Environment (LE) and z/OS UNIX System Services API SENDMSG has a new option called `ip_qos_classification_data`. It is for ancillary data. The `sendmsg()` API extensions are only applicable to the z/OS Language Environment (LE) and z/OS UNIX System Services APIs. They are not supported for some APIs, including the EZASMI macro API, Call instruction API, REXX sockets, PASCAL sockets, CICS and IMS sockets.

Restrictions

There are no restrictions.

What this change affects

- Customization
- Performance

Migration procedures

If you want to take advantage of the application-driven policy classification function, perform the task in the following table.

Table 62. Application-driven policy classification - Migration task

Task	Procedure	Reference
Define service policies using application provided classification data.	Specify application data and/or an application priority attribute in service policy rules.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Virtual LAN priority tagging

In z/OS V1R2 Communications Server, Quality of Service user priorities that are assigned to IP packets based on policy definitions can be mapped to user priorities on directly attached LANs. This means that when the Type of Service (ToS) byte, also known as the Differentiated Services (DS) field, is assigned to outbound IP packets using service policy definitions, the ToS/DS values can be mapped to user priorities for directly attached LANs. This allows assigned user priorities to be propagated through such networks, resulting in no loss of priority information for data being served by z/OS.

Restrictions

You must be running on IBM @server zSeries 900 Driver level 3C to use this function. It requires z/OS V1R2 OSA-Express hardware and microcode upgrade at 3C level.

Dependencies

This function is only available for an OSA-Express configured in QDIO mode.

What this change affects

- Customization
- Performance

Migration procedures

If you want to take advantage of the VLAN priority tagging function, perform the task in the following table.

Table 63. VLAN priority tagging - Migration task

Task	Procedure	Reference
Define outbound ToS/DS to user priority mappings.	Specify user priorities for directly attached LANs, which are mapped from the ToS/DS value for outbound IP packets, on the Policy Agent configuration statement or LDAP object SetSubnetPrioTosMask, using the PriorityTosMapping parameter.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Packet trace enhancements

In z/OS V1R2 Communications Server, the CTRACE packet trace formatter was rewritten to provide additional reports and outputs, including:

- A one-line summary report
- Rewritten formatters for application packet data
- Additional statistical reports
- Reassembly of IP packets session reports
- Reformatted trace data for input to Network Associates' Sniffer Pro
- Export of trace data that can be used for additional analysis

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

There are no migration tasks for the packet trace enhancements function; it is automatically enabled.

Fast connection reset for Sysplex Distributor

The fast connection reset after system failure function is an enhancement to Sysplex Distributor (introduced in OS/390 V2R10; see “Sysplex Distributor” on page 135) and VIPA Takeover (introduced in OS/390 V2R8). This enhancement allows the client stack to notify the client application of a system failure of a sysplex target stack for the distributed DVIPAs being maintained by the routing stack. This improves availability and allows quicker initiation of connection failure recovery. Prior to this release, the client was unaware of a system failure until it attempted to send data.

Restrictions

This enhancement only applies to the sysplex stacks for the distributed DVIPAs being maintained by the routing stack.

What this change affects

- Operations
- Availability

Migration procedures

There are no migration procedures for the fast connection reset after system failure enhancement. It is automatically enabled.

HiperSockets

HiperSockets is a zSeries hardware feature that provides very high-speed, low-latency IP message passing between Logical Partitions (LPARs) on the same processor complex (CEC). (Latency is the time interval between the instant when a call for data is initiated and the instant when the data transfer is completed.) It is an interface to device driver software and is similar to the Queued Direct I/O interface used with the OSA-Express adapter with Fast Ethernet and Gigabit Ethernet.

Note: HiperSockets is also known as Internal Queued Direct I/O, or iQDIO.

APAR OW49475 enables HiperSockets.

In z/OS V1R2 Communications Server, HiperSockets links are created and activated by two different functions:

- When Dynamic XCF is enabled. (This requires no additional configuration.)
- When a HiperSocket (iQDIO) MPCIPA device is configured.

Neither type (dynamic or configured) of HiperSocket devices requires a VTAM TRLE definition. The HiperSocket TRLEs are dynamically created.

Dynamic XCF can be enabled even when the z/OS is not in a parallel sysplex. Likewise, HiperSockets may be used between LPARs on the same CEC even when z/OS systems in those LPARs are not defined to be part of the same sysplex, or even when some of those other LPARs are running Linux. This is true if all of the stacks exchanging IP packets with each other are connecting to HiperSockets and have defined IP addresses in the same subnet.

For non-sysplex traffic, as another option, users can configure an MPCIPA HiperSocket (iQDIO) device (or devices). This approach allows users to isolate sysplex related traffic from non-sysplex related traffic using unique HiperSockets CHPIDs (LANs).

Refer to *z/OS Communications Server: IP Configuration Guide* for an in-depth discussion of the new HiperSockets function.

Restrictions

The HiperSockets function is only allowed if the following requirements are met:

- Subchannel addresses must be configured by IQD CHPID. A minimum of three is required; ten is the maximum allowed. The iQDIO subchannel devices associated with the selected IQD CHPID will be grouped together into a single MPC group (two read/write control devices and up to eight data devices). The subchannel devices must be online.
- HiperSockets can only be used between Logical Partitions on the same processor complex (CEC).
- Processor hardware support provided by the IBM @server zSeries 900 Driver level 3C. HiperSockets routing requires z/OS V1R2, hardware and microcode upgrade at 3C level. The hardware support is automatically detected and used when present. The start option IQDCHPID, and therefore, HiperSockets communications, cannot be specified, modified, or displayed on a processor without the hardware support.

Refer to *z/OS Communications Server: IP Configuration Guide* for more information on all the HiperSockets restrictions.

What this change affects

- Diagnosis
- Operations
- Performance

Migration procedures

The following table includes the IP, VTAM, and z/OS migration considerations for the HiperSockets function. The tasks are optional and do not require any action unless you want to take advantage of the function.

Table 64. HiperSockets - Migration tasks

Task	Procedure	Reference
Define the IQD CHPID and subchannel devices.	Using HCD, define the IQD CHPID and subchannel devices.	<i>z/OS HCD Planning</i>
Select the Dynamic XCF IQD CHPID for your LPAR.	Code the VTAM start option IQDCHPID = chpid.	<i>z/OS Communications Server: SNA Resource Definition Reference</i>
Change the IQD CHPID specification after VTAM is active (if not already defined in your VTAM start options).	Issue the MODIFY VTAMOPTS command.	<i>z/OS Communications Server: SNA Operation</i>
Enable Dynamic XCF.	Specify IPCONFIG DYNAMICXCF.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Table 64. HiperSockets - Migration tasks (continued)

Task	Procedure	Reference
Optionally, if more connectivity is desired, configure HiperSockets for non-Dynamic XCF connectivity.	Configure an MPCIPA device and link statement. Use the reserved name "IUTIQDxx" where xx equals the desired (hexadecimal) IQD CHPID (for example, 'FD'x).	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Determine if HiperSockets connectivity is being used.	Use PING to verify connectivity. Use NETSTAT to display the HiperSocket devices and links. Use VTAM display to display the associated HiperSocket TRLEs. Use VTAM tuning statistics to monitor traffic statistics.	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: SNA Operation</i>
Trace HiperSockets network traffic (packets).	Use the standard service aids. Qualify tracing by using the IPAQIDIO link type in Packet trace. The standard VTAM service aids can also be used (for example, VTAM IO trace or VIT (option = CIA)).	<i>z/OS Communications Server: IP User's Guide and Commands</i> , <i>z/OS Communications Server: SNA Operation</i> , and <i>z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures</i>
Migrate dynamic XCF interfaces to HiperSockets.	<p>If you are using OSPF, consider the following:</p> <ul style="list-style-type: none"> • Because dynamic XCF is a point-to-multipoint medium and HiperSockets is a broadcast medium (as far as OSPF is concerned because it supports multicast, which is the only kind of broadcast used by OSPF), your OSPF_INTERFACE definitions that currently represent the XCF links may need updating. If any of these OSPF_INTERFACE statements contain a wildcard IP address and will now represent a HiperSockets link instead of an XCF link, then you need to ensure that at least one host on the HiperSockets network has a nonzero ROUTER_PRIORITY defined for the OSPF_INTERFACE statement, so that a designated router can be elected on the HiperSockets network. Note that the default value for ROUTER_PRIORITY is 1 so if you do not have that parameter specified, you do not need to add it. Also ensure that none of the hosts on the HiperSockets network have NON_BROADCAST=YES defined on these OSPF_INTERFACE statements that will now represent a HiperSockets link. <p>If you are using RIP, consider the following:</p> <ul style="list-style-type: none"> • Because HiperSockets supports multicast but not broadcast, use of RIP2 is recommended. RIP2 uses multicast and RIP1 uses broadcast. <p>If you are using static routes, consider the following:</p> <ul style="list-style-type: none"> • Because HiperSockets uses a different linkname than XCF links, you may need to update your BEGINROUTES or GATEWAY statements. 	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: SNA Operation</i>

Efficient routing using HiperSockets Accelerator

z/OS V1R2 Communications Server introduces an improvement in performance when routing IP traffic between HiperSockets (also known as Internal Queued Direct Input/Output or iQDIO) and Queued Direct I/O (QDIO). This type of routing is called *HiperSockets Accelerator* because it allows you to concentrate external network traffic over a single OSA-Express QDIO connection and then accelerates (speeds up) the routing over a HiperSockets link bypassing the TCP/IP stack (IP Forwarding process).

Specifically, HiperSockets Accelerator allows a large number of system images on one CEC, such as zSeries Linux images, to access a resource with limited channel address capability, such as an OSA-Express. It does so by allowing one z/OS CS image to have access to the resource and by creating highly optimized routes from that one z/OS CS image to and from other system images using HiperSockets devices. These new highly optimized routes allow data to be routed through the HiperSockets devices with minimal processing by the TCP/IP stack and without exhausting the channel address limitation of the OSA-Express.

Refer to *z/OS Communications Server: IP Configuration Guide* for an in-depth description of HiperSockets and HiperSockets Accelerator.

Restrictions

The following restrictions apply:

- You must be running on IBM @server zSeries 900 Driver level 3C to use this function. HiperSockets Accelerator requires z/OS V1R2, hardware and microcode upgrade at 3C level.
- HiperSockets Accelerator cannot be used when Firewall is active.
- HiperSockets Accelerator cannot be used unless IP forwarding is specified (DATAGRAMFWD).
- HiperSockets Accelerator is only supported for IPV4 packets with no IP options.
- HiperSockets Accelerator can only be used when no fragmentation is required.
- HiperSockets Accelerator will be used only for unicast packets (no broadcast or multicast packets can be routed over HiperSockets routes).

Dependencies

The following dependencies apply:

- HiperSockets must be available on the host system.
- If data inbound from MPCIPA devices is to use HiperSockets Accelerator, PRIROUTER must be specified on the MPCIPA device.

What this change affects

- Customization
- Diagnosis
- Operations
- Performance

Migration procedures

If you want to take advantage of the efficient routing using HiperSockets Accelerator, perform the tasks in the following table.

Table 65. Efficient routing using HiperSockets Accelerator - Migration tasks

Task	Procedure	Reference
Enable the usage of HiperSockets.	See Table 64 on page 115 for the steps necessary to enable HiperSockets.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Enable HiperSockets Accelerator.	Specify the IQDIORouting parameter on the IPCONFIG statement in the TCP/IP profile. Optionally specify a QDIOPriority value.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Connection load balancing using Sysplex Distributor in a network with Cisco routers

Sysplex Distributor was introduced in CS for OS/390 V2R10 (see “Sysplex Distributor” on page 135). z/OS V1R2 Communications Server enhances Sysplex Distributor to work in conjunction with Cisco’s MultiNode Load Balancing (MNLB).

Cisco’s MNLB consists of a Service Manager (the Cisco Local Director, which is denoted by a cluster IP address) and a set of Forwarding Agents (Cisco routers). The Cisco Service Manager requires local director (LD) hardware. As a result of this z/OS V1R2 Communications Server enhancement, Sysplex Distributor can now perform the Service Manager function for MNLB for any desired distributable Dynamic VIPAs.

You can use a combination of the Sysplex Distributor and Cisco’s forwarding agents to provide workload balancing. This provides a way to avoid having all inbound traffic flow through a single node. In addition, this enhancement supports Generic Routing encapsulation (GRE). This means that the first time a packet is routed, it must go through Sysplex Distributor, but subsequent packets can bypass the Sysplex Distributor and go directly to the target stack, thereby improving performance.

For details on how to configure the Cisco MNLB, refer to Cisco publications. At the time of this writing, the Cisco publication *MultiNode Load Balancing Feature Set for Local Director User Guide* can be found at <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/localdir/mnlb/index.htm>. The “Configuring the MNLB Services Manager” chapter describes how to configure a Cisco LocalDirector as the MNLB Service Manager. The “Configuring the MNLB Forwarding Agent” chapter describes how to configure a Cisco router as an MNLB Forwarding Agent.

Restrictions

The following restrictions apply:

- UDP is not supported. Like the Sysplex Distributor of CS for OS/390 V2R10, this enhancement only provides workload balancing for TCP connections.
- A TCP/IP stack performing VIPABACKUP for a dynamic VIPA that has the SERVICEMGR function must be at a z/OS CS V1R2 level. If the backup stack is at a lower level, then after Dynamic VIPA takeover, data destined for the distributed VIPA may be lost.
- A TCP/IP stack that is a target for a dynamic VIPA that has the SERVICEMGR function must be at a z/OS CS V1R2 level to obtain the performance improvements of Service Manager. If the target stack is CS for OS/390 V2R10,

sysplex distribution will work; however, the routing must be configured so the selected route from the CS for OS/390 V2R10 target to the z/OS CS V1R2 routing stack is not through the CISCO MNLB service manager for this Distributed VIPA. Furthermore, performance will be degraded.

Dependencies

The following dependencies apply:

- For the SERVICEMGR function to work properly for Dynamic VIPAs, the sysplex must be entirely front-ended by forwarding agents. In other words, if routers that cannot act as forwarding agents lie between the routers that can act as forwarding agents and the target stacks, then routing to the destination target stacks may not work properly.
- If two or more TCP/IP stacks that are targets for Dynamic VIPA addresses with the SERVICEMGR function share the same OSA adapter, GRE tunnels must be used. A GRE tunnel to the dynamic XCF address of each target stack sharing the OSA adapter must be configured on the Cisco Router.
- Special consideration must be made for each target stack that will receive data from an OSA that is *not* shared with the distributor. Either GRE tunnels must be used or PRIROUTER must be specified on the OSA DEVICE MPCIPA definition of each target stack. A GRE tunnel to the dynamic XCF address of each target stack must be configured on the Cisco router.

What this change affects

- Customization
- Availability
- Usability
- Performance

Migration procedures

If you want to take advantage of the connection load balancing using Sysplex Distributor in a network with Cisco routers function, perform the tasks in the following table.

Table 66. Connection load balancing using Sysplex Distributor in a network with Cisco routers - Migration tasks

Task	Procedure	Reference
Use the Sysplex Distributor in conjunction with the Cisco MultiNode Load Balancer (MNLB).	Specify the SERVICEMGR keyword on the VIPADEFine statement in the TCPIP profile. Specify the same multicast group and UDP port on the VIPASMParms statement in the TCPIP profile as are configured in the MNLB.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Use MD5 authentication when Sysplex Distributor is used with the MNLB.	Specify the same MD5 password on the VIPASMParms statement in the TCPIP profile as is configured on the Cisco routers.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Use the Cisco MNLB in a configuration where there is an OSA in between a Cisco router and the destination TCP/IP stacks such that multiple stacks are sharing the OSA.	Configure GRE tunnels on the Cisco routers.	<i>z/OS Communications Server: IP Configuration Guide</i> and Cisco documentation mentioned in the description section of this function.

Table 66. Connection load balancing using Sysplex Distributor in a network with Cisco routers - Migration tasks (continued)

Task	Procedure	Reference
Use the Cisco MNLB in a configuration where there is an OSA in between a Cisco router and the destination TCP/IP stacks such that multiple stacks are NOT sharing the OSA.	Configure GRE tunnels on the Cisco routers or specify PRIROUTER on the DEVICE MPCIPA definition on each target stack.	<i>z/OS Communications Server: IP Configuration Reference</i> , <i>z/OS Communications Server: IP Configuration Guide</i> , and Cisco documentation mentioned in the description section of this function.

CICS sockets listener enhancements

z/OS V1R2 Communications Server enhances the CICS sockets listener to allow more flexibility in scheduling CICS transaction using TCP/IP sockets while minimizing changes required by the client applications. Specifically, the enhancements for CICS sockets listener include the following changes:

- A standard CICS sockets message header (Transaction Request Message) no longer needs to be present in the first message sent by the client application. The information that was previously obtained by use of this message header, such as the CICS transaction to be run, can now be specified in the CICS Sockets Listener configuration for a given TCP port.
- The CICS socket listener security exit has been enhanced to allow users to also use it as a transaction scheduling exit. This exit can now be used to determine which CICS transaction should be scheduled for an incoming TCP connection based on information such as the client's IP address or based on the contents of the first message received from the client.

These enhancements allow users to create new CICS sockets applications that service existing client TCP/IP socket applications without any modifications on the client end. This can be particularly useful in scenarios where a CICS sockets application is deemed as an ideal solution yet the installation has little control or desire to make modifications to the client applications.

Restrictions

None.

What this change affects

- Customization
- Application Development
- Usability

Migration procedures

If you want to take advantage of the CICS sockets listener enhancements, perform the tasks in the following table.

Table 67. CICS sockets listener enhancements - Migration tasks

Task	Procedure	Reference
Use an enhanced CICS listener instead of the standard CICS listener.	Convert standard listeners to enhanced listeners by using the EZAC, CONVERT, LISTENER command (and specifying "ENHANCED" at the "FORMAT" prompt), or by recoding the EZACICD TYPE=LISTENER macro using the "FORMAT=ENHANCED" option.	<i>z/OS Communications Server: IP CICS Sockets Guide</i>

Table 67. CICS sockets listener enhancements - Migration tasks (continued)

Task	Procedure	Reference
Interpret new listener output.	Update any child server applications started by a listener that has been converted from standard to enhanced to specify a large enough length on the EXEC CICS RETRIEVE or EXEC CICS READQ TD command used to receive the TIM.	<i>z/OS Communications Server: IP CICS Sockets Guide</i>
Interpret new Security/Transaction exit data.	Pass the following: <ul style="list-style-type: none"> • The listener's IP address and port number • A data length field • A larger amount of data (up to the MSGLENTH value) Recognize the new indicator indicating the expanded Security/Transaction input format is being used so that the same Security/Transaction exit program can run with both the enhanced and standard versions of the listener.	<i>z/OS Communications Server: IP CICS Sockets Guide</i>
Remove FASTRD from EZACICD macro.	Remove the FASTRD parameter from the EZACICD macro in order to avoid generating an MNOTE that indicates that the FASTRD parameter is obsolete.	<i>z/OS Communications Server: IP CICS Sockets Guide</i>

SMF recording enhancements

z/OS V1R2 Communications Server enhances System Management Facilities (SMF) recording to provide additional SMF information about stack and application processing and to provide it in a more standardized format. Prior to z/OS V1R2 Communications Server, SMF records had differing content formats which were often difficult to expand with new information. In addition, the records did not have an easy mechanism for connecting one SMF record to a given TCP/IP stack running. The z/OS V1R2 Communications Server SMF records have formats that are easy to expand and they include a common TCP/IP Stack Identification section for quick identification of the issuing stack.

Refer to *z/OS Communications Server: IP Configuration Guide* for more information about the SMF recording enhancements.

Additional considerations

SMF format type 118 records existed prior to this release and the formats are unchanged. Two fields, however, are modified to show a more precise value. Specifically, the TCP Connection Initiation and Termination records have start and end timestamps, which previously were cut when the related job started and the connection control block was cleaned up, respectively. This gave an exaggerated view of how long the connection lasted. The timestamps now reflect when the connection was available for data transfer and when the connection was no longer available for data transfer, respectively.

Restrictions

None.

Incompatibilities

System performance might be impacted in a negative way if the current TCP/IP SMF records are collected in addition to the new records.

What this change affects

- Operations
- Performance

Migration procedures

SMF format type 118 records existed prior to this release and there are no migration procedures associated with using it. This enhancement introduces format type 119. If you want to take advantage of the SMF recording enhancements, perform the tasks in the following table.

Table 68. SMF recording enhancements - Migration tasks

Task	Procedure	Reference
Allocate the SMF data set and set up the MVS SMF parameters as necessary to allow a collection of type 119 records.	Use the DSNNAME parameter in the SMFPRMxx parmlib member. Specify SYS(TYPE(119)) on the same SMFPRMxx member. Use the INTVAL or SYNCVAL operands to specify the SMF interval, if interval records are desired.	<i>z/OS MVS System Management Facilities (SMF)</i>
Enable collection of desired new format 119 SMF records.	Code required operands on the SMFCONFIG or TELNETPARMS statements in the CONFIG profile, or in the FTP.DATA file.	<i>z/OS Communications Server: IP Configuration Reference</i>
Disable current format 118 SMF recording (optional, but recommended).	Remove existing operands on the SMFCONFIG or TELNETPARMS statements in CONFIG profile, or in FTP.DATA file.	<i>z/OS Communications Server: IP Configuration Reference</i>
Verify that the format 119 SMF options are enabled correctly.	Use netstat CONFIG or onetstat -f commands.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Interpret SMF records.	Utilize EZASMF77 to get the correct mappings of the new records.	<i>z/OS Communications Server: IP Configuration Reference</i>
If the FTP user exit FTPSMFEX was used to process format 118 records, modify the SMF system-wide user exit to perform a similar function for format 119 records.	Add code to the system exit.	<i>z/OS Communications Server: IP Configuration Reference</i>

SMTP exit to filter unwanted mail

z/OS V1R2 Communications Server introduces enhancements to the Simple Mail Transfer Protocol (SMTP) exit. If you are using the SMTPPROC application that was supplied with your installation, you can now design an SMTP exit to inspect and filter mail sent through SMTPPROC, thus controlling the influx of unwanted or harmful mail (commonly referred to as *spam*) into your network. This is a benefit because it allows the exit to refuse these items (based on criteria you define) before they consume processing, storage, and human time resources. Additionally, one of the features of the SMTP exit is that it can be replaced dynamically without stopping the SMTPPROC program.

A sample assembler exit is provided by IBM as a programming guide to aid in the implementation of the local policies. The sample is called SMPTEXTIT and can be found in the EZBZSMTP macro.

Restrictions

None.

What this change affects

- Operations
- Performance

Migration procedures

If you want to write an SMTP exit to filter unwanted mail, perform the tasks in the following table.

Table 69. SMTP exit to filter unwanted mail function - Migration tasks

Task	Procedure	Reference
Design the new SMTP exit to control the influx of unwanted mail into your network.	Study the sample program and RFC 2505 and RFC 2635 for hints and directional information.	<i>z/OS Communications Server: IP Configuration Reference</i> , <i>z/OS Communications Server: IP Configuration Guide</i> , and <i>z/OS Communications Server: IP User's Guide and Commands</i>
Replace the SMTP exit dynamically without stopping the SMTPPROC program.	Do the following: <ul style="list-style-type: none">• Issue a "MSG smtpprocname STOPEXIT" TSO command.• Remove the exit by using the SETPROG EXIT operator command or by updating SYS1.PARMLIB(PROGxx) and issuing the refresh console command.• Replace the old exit with the desired new exit and add the exit by using the SETPROG EXIT operator command or by updating SYS1.PARMLIB(PROGxx).• Issue a "MSG smtpprocname STARTEXIT" TSO command.	<i>z/OS Communications Server: IP System Administrator's Commands</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Managed System Infrastructure (msys) for Setup

z/OS V1R2 Communications Server supports Managed System Infrastructure for Setup (msys for Setup). msys for Setup is a configuration tool for customizing z/OS using GUI panels on a workstation rather than the traditional means of editing data sets directly on the mainframe and specifying configuration statements and parameters directly into these files. Once a system has been customized by using msys for Setup, the customized data is stored into an LDAP directory for reuse. The benefit of using msys for Setup is that it helps system administrators keep track of various configuration data sets by establishing a central directory for product configuration data and a single interface to this directory.

To use msys for Setup, you must install it and set it up on the workstation. Additionally, msys for Setup requires a significant MVS driving system already up and running. Refer to *z/OS Managed System Infrastructure for Setup User's Guide* for complete information.

Restrictions

Using msys for Setup will not provide as much flexibility for customization as the traditional editing of configuration data sets. Furthermore, msys for Setup does not provide a migration of existing TCP/IP customer configurations.

Dependencies

z/OS CS requires the msys for Setup base, which has a separate FMID. Other z/OS elements exploit msys for Setup, but are not required to run TCP/IP's msys for Setup base.

What this change affects

- Customization
- Installation
- Usability

Migration procedures

If you want to take advantage of the msys for Setup function, perform the task in the following table.

Table 70. msys for Setup - Migration task

Task	Procedure	Reference
Install and set up msys for Setup both on the mainframe and workstation.	Refer to the procedures in <i>z/OS Managed System Infrastructure for Setup User's Guide</i> .	<i>z/OS Managed System Infrastructure for Setup User's Guide</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Improve TCP/IP storage utilization management

z/OS V1R2 Communications Server provides several enhancements for more effective monitoring and management of storage used by TCP/IP. These enhancements allow you to do the following:

- Monitor TCP/IP storage usage with a new operator command. This command displays the amount of Common (CSA) storage and authorized subpool private storage that TCP/IP is utilizing, including high water mark usage to identify peak workload storage utilization. This data can be very helpful in capacity planning for storage.
- Set limits on the amount of CSA and authorized subpool private storage that TCP/IP can utilize. These limits are automatically monitored by TCP/IP and messages are issued when these resources become constrained. Note that these new limits are not tuning controls for TCP/IP, rather they are defensive controls that can be used to help avoid overall system failures as a result of TCP/IP using excessive amounts of common or private storage. For proper TCP/IP operations, sufficient storage needs to be available. Therefore, it is recommended that users perform a careful examination of their system's TCP/IP storage requirements prior to specifying these storage limits.

Restrictions

None.

What this change affects

- Customization
- Operations
- Diagnosis
- Availability
- Storage

Migration procedures

If you want to take advantage of the improve TCP/IP storage utilization management function, perform the tasks in the following table.

Table 71. Improve TCP/IP storage utilization management function - Migration tasks

Task	Procedure	Reference
Display TCP/IP storage usage information.	Issue the D TCPIP,,STOR command.	<i>z/OS Communications Server: IP Configuration Reference</i>
To improve system reliability, establish a limit on total amount of TCP/IP common storage.	Run the system without any limit, and issue the D TCPIP,,STOR command to see the maximum ECSA usage. Allow additional storage for future growth and then establish a limit in the TCP/IP profile with a GLOBALCONFIG ECSALIMIT statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Establish a limit on the amount of TCP/IP's use of private storage.	Specify the GLOBALCONFIG POOLLIMIT statement.	<i>z/OS Communications Server: IP Configuration Reference</i>

Enterprise Extender performance enhancements

z/OS V1R2 Communications Server enhances the performance of Enterprise Extender by reducing the pathlength of route lookups for EE traffic when the destination IP address changes. There are no migration procedures or changed interfaces as a result.

Restrictions

None.

What this change affects

- Performance

Migration procedures

There are no migration procedures.

Enhanced CLAW packing

In CS for OS/390 V2R10, CLAW performance was improved for small MTU traffic when CS for OS/390 was communicating with Cisco 7200-series and 7500-series routers (see “CLAW packing within a 4K frame” on page 164). z/OS V1R2 Communications Server enhances the CLAW support to fully exploit the Datagram Packing feature of the Cisco 7200 and 7500 series routers. While CS for OS/390 V2R10 limited buffer size to 4K, z/OS V1R2 Communications Server allows for buffer sizes of up to 60 KB.

The z/OS V1R2 Communications Server Enhanced CLAW Packing function provides a significant performance improvement over prior releases. Specifically, throughput is increased and CPU consumption is reduced because the ESCON overhead involved in CLAW communications is reduced.

To enable this feature, you must update the CLAW device statement in the PROFILE.TCPIP. You must also update the CLAW statement within the Cisco router.

Restrictions

None.

What this change affects

- Customization
- Performance

Migration procedures

If you want to take advantage of the enhanced CLAW packing function, perform the tasks in the following table.

Table 72. Enhanced CLAW packing function - Migration tasks

Task	Procedure	Reference
Determine if packed mode for CLAW is supported in your configuration.	Packed mode for CLAW is supported only when z/OS is communicating with Cisco 7200 series or 7500 series routers.	Refer to the CLAW DEVICE statement in <i>z/OS Communications Server: IP Configuration Reference</i> to determine the prerequisite Cisco microcode levels or contact the Cisco Support group.
If, in the previous step, you concluded packed mode is supported in your configuration, enable packing for z/OS CS and for the Cisco router.	On the z/OS CS side, specify the PACKED keyword on the CLAW DEVICE statement. On the Cisco side, enable packing on the CLAW statement for the CIP interface. If you were using CLAW packing in releases prior to z/OS CS V1R2, update your PROFILE.TCPIP to specify CLAW WRITE and READ buffer sizes of at least 32K. z/OS CS V1R2 raises the minimum buffer size for packed mode to 32K and it issues a message if you attempt to configure a buffer size smaller than this.	Refer to the CLAW DEVICE statement in <i>z/OS Communications Server: IP Configuration Reference</i> . Refer to Cisco documentation for the CLAW statement syntax within the Cisco router.
If, in the first step, you concluded packed mode is not supported in your configuration, operate in non-packed mode.	You do not need to change anything to operate in non-packed mode; NONE is the default for the CLAW DEVICE statement and it runs the device in non-packed mode.	Refer to the CLAW DEVICE statement in <i>z/OS Communications Server: IP Configuration Reference</i> .

64-bit real addressing support

TCP/IP exploits real storage in excess of 2 gigabytes by allowing z/OS to back most fixed CSM data space pages on or above the 2-gigabyte real storage bar. This enhances performance when z/OS V1R2 Communications Server is executing in z/Architecture™ mode.

Refer to *z/OS Communications Server: SNA Migration* for more information on 64-bit real addressing support, including SNA Migration tasks and changed interfaces.

Restrictions

64-bit real storage support is only enabled when the machine is executing in z/Architecture mode.

Note: Specifying ARCHLVL 2 in LOADxx in SYS1.PARMLIB enables z/Architecture mode.

Additional considerations

CSM data space will be backed by 64-bit real storage when the machine is in z/Architecture mode. This storage may be passed to applications. If these applications attempt to issue the LRA (Load Real Address) instruction on this storage, a special operation exception program interrupt may occur. However, this is highly unlikely because LRA is primarily used to determine real addresses in preparation of structures used in I/O operations. There is no known application that performs I/O to or from received CSM data space storage. If an application accepts CSM data space and determines the data should be saved on external media, the data is usually copied to primary storage then passed to an access method. IBM recommends building a test environment that includes all applications to be used.

What this change affects

- Performance

Migration procedures

The 64-bit real addressing support function does not require any action; it is automatically enabled at initialization time for z/OS V1R2 Communications Server when the system is executing in z/Architecture mode. It cannot be disabled. However, you can control whether or not your application programs are passed 64-bit backed storage by using the new API64R start option. Refer to *z/OS Communications Server: SNA Resource Definition Reference* for more information about the API64R start option.

Table 73. 64-bit real addressing support - Migration tasks

Task	Procedure	Reference
Build a test environment that includes all applications to be used.	Start z/OS CS and initiate application activity. Observe any 00D3 system abends that occur. If a 00D3 system abend occurs, determine if the OpCode causing the abend is X'B1'. If so, notify the applications support group of the abend. Until the applications are updated, code API64R=NO to alleviate the 00D3 system abends.	<i>z/OS Communications Server: SNA Resource Definition Reference</i>

OSA-Express token ring support

z/OS V1R2 Communications Server provides for support of an OSA-Express with token ring attachment, allowing users of OSA-Express access to either 16M or 100M token ring networks. Users with access to token ring networks may now take advantage of the highly optimized data-transfer interface of Queued Direct I/O. Among the advantages of Queued Direct I/O are the IP Assist features of Address

Resolution Protocol (ARP) Offload, packet filtering, MAC handling by the OSA-Express, OSA-Express routing, and the use of the Self-Timed Interconnect (STI) bus. Prior to this support, users with token ring networks could not use high speed token ring switches because OSA-Express has no token ring attachment and OSA-2 only has support for 4M or 16M switches.

z/OS V1R2 Communications Server also allows defining the OSA-Express as an LCS device. This option allows you to migrate from your existing OSA token ring attachments to OSA-Express without changing your profile definitions, but without the advantages of Queued Direct I/O.

Restrictions

You must be running on IBM @server zSeries 900 Driver level 3C to use this function. It requires the OSA-Express hardware and microcode upgrade at 3C level.

What this change affects

- Customization
- Operations
- Usability
- Performance

Migration procedures

If you want to take advantage of the OSA-Express token ring support, perform the tasks in the following table.

Table 74. OSA-Express token ring support - Migration tasks

Task	Procedure	Reference
Use the OSA-Express with token ring attachment as an LCS device.	Use LCS definitions identically to using an OSA-2 adapter with token ring attachment.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Table 74. OSA-Express token ring support - Migration tasks (continued)

Task	Procedure	Reference
Use the OSA-Express with token ring attachment in Queued Direct I/O Mode.	Define the CHPID for the OSA-Express as OSD.	<i>zSeries: OSA-Express Customer's Guide and Reference</i>
	Define a TRLE to represent the OSA-Express token ring adapter. It must include MPCLEVEL of QDIO, PORTNAME, one or more DATAPATH addresses, and one READ and one WRITE address.	<i>z/OS Communications Server: SNA Resource Definition Reference</i>
	Define a DEVICE statement of type MPCIPA and a LINK statement of type IPAQTR. Ensure the DEVICE name matches the PORTNAME on the TRLE statement above. Specify PRIROUTER, SECROUTER, or NONROUTER as desired.	<i>z/OS Communications Server: IP Configuration Reference</i>
	If the default mapping of the Type of Service (ToS) byte to QDIO priority levels is insufficient, define a SetSubnetPrioTosMask statement to map the ToS byte to particular QDIO priority levels.	<i>z/OS Communications Server: SNA Network Implementation Guide and z/OS Communications Server: IP Configuration Reference</i>
	For static routes, either code GATEWAY statements using a next hop IP address on the token ring, or use the BEGINROUTES statement. For OMPROUTE, use OSPF_Interface statements if OSPF is the routing protocol being used, or RIP_Interface statements if RIP is the routing protocol being used. Note that jumbo frames are not supported for token ring.	<i>z/OS Communications Server: IP Configuration Reference</i>

Changes to EZAZSSI

In z/OS CS V1R2, the restartable VMCF/TNF sample started procedure, EZAZSSI, is changed. The nodename parameter, P=, will now default to the value of the MVS system symbolic &SYSNAME. If the name you are currently specifying for the P= parameter when you issue the S EZAZSSI command is the same as the &SYSNAME value, then you no longer have to specify the P= parameter when starting EZAZSSI.

Restrictions

None.

What this change affects

- Customization
- Operation

Migration procedures

Table 75. Changes to EZAZSSI - Migration task

Task	Procedure	Reference
Start restartable VMCF/TNF.	If name specified on the P= parameter is the same as the &SYSNAME value, issue the S EZAZSSI command without the P= parameter.	<i>z/OS Communications Server: IP Configuration Guide</i>

IPSec enhancements

In releases prior to z/OS V1R2 Communications Server, Path MTU Discovery was not allowed when using IPSec connections. z/OS V1R2 Communications Server provides this capability, thus allowing the optimization of the size of the data sent and the reduction of fragmentation, reassembly, and retransmissions.

IPSec tunnels using AH in tunnel mode and ESP in transport mode are not supported in z/OS CS V1R2. Dynamic tunnels configured using AH in tunnel mode and ESP in transport mode will fail to negotiate. Refer to *z/OS Security Server Firewall Technologies* for more information on dynamic tunnels.

Restrictions

None.

What this change affects

- Performance

Migration procedures

If you want to take advantage of the IPSec performance enhancements, perform the task in the following table.

Table 76. IPSec performance enhancements - Migration task

Task	Procedure	Reference
Enable Path MTU Discovery support for IPSec connections.	Specify the IPCONFIG PATHMTUDISCOVERY profile statement.	<i>z/OS Communications Server: IP Configuration Reference</i>

TCP configuration options

z/OS V1R2 Communications Server includes enhancements to the TCP TIMESTAMP option and to the FINWAIT2 configurable timer.

The TCP timestamp option is exchanged during the connection setup. If it is enabled (by default) in the profile and z/OS TCP/IP initiates a TCP connection, then a TCP timestamp option will be sent as per RFC 1323. When this option is enabled during a passive connect, such as when z/OS TCP/IP receives a TCP connection request carrying a TCP timestamp option from a client, the z/OS TCP/IP stack will send a SYN-ACK with its own TCP timestamp option as per RFC 1323. Enabling the TCP timestamp option allows TCP/IP to better estimate the Round Trip Response Time (RTT), which helps avoid unnecessary retransmissions and helps protect against wrapping of sequence numbers. This is most beneficial when using very high speed networks. If this option is disabled, the z/OS CS TCP/IP stack will not participate in TCP timestamp negotiation during connection setup or during the lifetime of the connection.

A TCP connection goes into a FINWAIT2 state when a FIN is acknowledged by the peer but the peer has not sent its own FIN to end the connection. In previous releases, in this situation a timer would have been started for 600 seconds (10 minutes 75 seconds) long. When this timer expired, an RST was sent to the peer. This enhancement makes this timer configurable with minimum of 60 seconds and a maximum of 3600 seconds. This reduces the amount of time a connection may remain in FIN_WAIT_2 state and frees up resources for future connections, thereby eliminating possible storage problems.

Restrictions

None.

What this change affects

- Performance

Migration procedures

If you want to take advantage of the TCP configuration options enhancements, perform the tasks in the following table.

Table 77. TCP configuration options enhancements - Migration tasks

Task	Procedure	Reference
Disable TCP Timestamp support.	Specify TCPCONFIG NoTCPTimeStamp Profile statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Modify TCP Finwait2 time value.	Specify TCPCONFIG FINWAIT2TIME Profile statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Display current TCP configuration values.	Specify Netstat CONFIG/-f option.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Chapter 7. z/OS V1R1 Communications Server release summary

| z/OS V1R1 Communications Server is identical in function to Communications
| Server for OS/390 V2R10; see Chapter 8, “Communications Server for OS/390
| V2R10 release summary” on page 135 for descriptions of the functions and
| enhancements introduced in that release, including migration considerations.

For complete information on z/OS Communications Server, see the z/OS Internet Library website: <http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>.

For complete information on Communications Server for OS/390, see the OS/390 Internet Library website: <http://www.s390.ibm.com/os390/bkserv/>.

Chapter 8. Communications Server for OS/390 V2R10 release summary

This chapter describes the major changes introduced in Communications Server for OS/390 V2R10.

See Table 15 on page 23 for a complete list of the functional enhancements you should consider. See Chapter 3, “New and changed interfaces” on page 29 for information on new, changed, deleted, or obsolete statements, commands, and APIs.

For information about changes to File Transfer Protocol (FTP), see Chapter 9, “Migrating the FTP server and client” on page 167.

For information about changes to Telnet, see Chapter 10, “Migrating the Telnet server and client” on page 203.

For information about changes to Simple Network Management Protocol (SNMP), see Chapter 11, “Migrating the SNMP server and client” on page 231.

For information about changes to Domain Name Server (DNS), see Chapter 12, “Migrating to the BIND-based DNS name server” on page 249.

When migrating, consider using the new BEGINROUTES statement instead of the GATEWAY statement in the PROFILE.TCPIP because it uses standard BSD syntax. Also, future enhancements to static route definitions are expected to be made to the BEGINROUTES statements only.

Note: As of OS/390 V2R10, IBM Communications Server no longer accepts 255.254 as a valid subnet mask. The smallest subnet mask value allowed is now 255.255.255.252. The value of 255.255.255.254 is no longer valid because of improved validation of outbound packets per RFC 1860. These addresses are now defined by using host route advertisements. All VIPAs in a sysplex can be defined in a single subnet and advertised as host routes.

CS for OS/390 V2R10 splits IP configuration information into two separate documents: *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*. Descriptions of the configuration documents are included in “Where to find related information on the Internet” on page xx.

Sysplex Distributor

The Sysplex Distributor function is a new function for CS for OS/390 V2R10 and it takes the XCF dynamics support in CS for OS/390 V2R7 and the Dynamic VIPA support in CS for OS/390 V2R8 to a whole new level in terms of availability and workload balancing in a parallel sysplex. By allowing a dynamic VIPA to become a sysplex wide VIPA address, workload can be distributed to multiple server instances without requiring changes to clients or networking hardware and without delays in connection setup. Because the Sysplex Distributor function resides in the parallel sysplex itself, it has the ability to factor in real-time information concerning the multiple server instances, including server status as well as QoS and Policy information provided by the Service Policy Agent of z/OS CS. By combining these real-time factors with the information obtained from Workload Management (WLM),

the Sysplex Distributor has the unique ability to ensure that the best destination server instance is chosen for a particular client connection while maintaining client/server specific Service Level Agreements.

Specifically, Sysplex Distributor provides the following capabilities:

- It routes client connection requests using a single IP address to servers on different mainframe hosts defined with an IPConfig DYNAMICXCF statement (Dynamic XCF). Routing to the server takes place over Dynamic XCF links; therefore connectivity of the server hosts to a single router is not required.
- Sysplex Distributor will query the policy repository to find if any policy defined for routing the incoming connection requests exists. If a policy is found, it will use the Dynamic XCF addresses specified in the policy for routing the requests.
- Workload Management (WLM) and/or Quality of Service (QoS) policy can be specified for workload balancing in real-time on every new connection request.
- It raises the limit of 64 DVIPA's on a stack to 256.
- Backup capability is provided by an enhancement to Dynamic VIPA Support (introduced in CS for OS/390 V2R8) in case of outages of the routing TCP/IP so that existing connections to other TCP/IPs in the sysplex are not disrupted.
- It provides workload distribution in a service provider environment by allowing different distribution points within the sysplex based on unique application/client load balancing requirements. The access to these distribution points can be totally independent from one another (such as different OSA Express Adapters).
- The new Netstat VCRT/-V and Netstat VDPT/-O options are added to display both the Connection Routing Table and Destination Port Table information. Both option reports can be filtered by either IP address or port number.

Refer to the discussion on Virtual IP Addressing in *z/OS Communications Server: IP Configuration Guide* for complete information.

Restrictions

IBM recommends that all TCP/IPs that may be participants in a Sysplex Distributor environment be at CS for OS/390 V2R10 or later because of the following restrictions:

- Workload distribution is only available when both the distributing and target stacks are at CS for OS/390 V2R10 or later.
- A CS for OS/390 V2R8 TCP/IP may back up a distributing Dynamic VIPA (DVIPA) but would be unable to distribute workload if the distributing stack was brought down. In this case, all workload would be processed by the CS for OS/390 V2R8 stack.

If you are using both CS for OS/390 V2R8 and CS for OS/390 V2R10 stacks in the same sysplex and they may back each other up, IBM recommends including the CS for OS/390 V2R8 stack's DVIPAs in the first 64 DVIPAs defined in the CS for OS/390 V2R10 stack.

If you are running the D TCPIP,,SYSPLEX,VIPAD command in a sysplex with mixed releases (such as CS for OS/390 V2R8 and CS for OS/390 V2R10), IBM recommends that you always run the command on the higher level systems. The lower level systems will not display all information for later releases. Specifically, it will not display any distribution related information and it will only display 64 DVIPAs per stack. If the current release's stack has more than 64 DVIPAs defined on it, a display from a previous release's stack will not reflect all of them.

Incompatibilities

Static IUTSAMEH definitions are incompatible with running Sysplex Distributor. Dynamic XCF will create all necessary IUTSAMEH links automatically.

The default behavior for dynamic DVIPAs defined in CS for OS/390 V2R10 is MOVEable IMMEDIATE. MOVEable IMMEDIATE now means the DVIPA will move immediately to the defining stack. The defining stack will forward packets to any existing connections before the takeover. This behavior is different than for DVIPAs defined previously. In CS for OS/390 V2R8, the defining stack would have to wait until the current owning stack finished processing all connections attached to it.

What this change affects

- Customization
- Operation
- Availability

Migration procedures

If you want to take advantage of the Sysplex Distributor function, perform the tasks in the following table.

Table 78. Sysplex Distributor - Migration tasks

Task	Procedure	Reference
Update the distributing stack's TCP/IP profiles.	<ul style="list-style-type: none"> • Add IPCONFIG DYNAMICXCF <i>ipaddr</i> to the TCP/IP profile for every stack that will distribute connections. • Add VIPADISTRIBUTE statement to the existing or new VIPADYNAMIC /ENDVIPADYNAMIC block in the profile for the selected distributing stack. • Specify IPCONFIG DATAGRAMFWD on all distributing stacks. • To use WLM, specify IPCONFIG SYSPLEXROUTING on all distributing and target stacks. 	<i>z/OS Communications Server: IP Configuration Reference</i>
Update the backup stack's TCP/IP profiles.	<ul style="list-style-type: none"> • Add IPCONFIG DYNAMICXCF <i>ipaddr</i> to the TCP/IP profile for every stack that will be a backup for a distributing stack. • Specify IPCONFIG DATAGRAMFWD on all distributing stacks. • To use WLM, specify IPCONFIG SYSPLEXROUTING on all distributing and target stacks. • Add an appropriate VIPABACKUP statement to all stacks that will backup the distributing stacks. 	<i>z/OS Communications Server: IP Configuration Reference</i>
Update the target stack's TCP/IP profiles.	<ul style="list-style-type: none"> • Add IPCONFIG DYNAMICXCF <i>ipaddr</i> to the TCP/IP profile for every stack that will be a target of a distributing stack. • To use WLM, specify IPCONFIG SYSPLEXROUTING on all distributing and target stacks. 	<i>z/OS Communications Server: IP Configuration Reference</i>
Use policy definition to control distribution of work.	Define Sysplex Distributor routing policies to the Policy Agent.	<i>z/OS Communications Server: IP Configuration Guide</i>
Display configuration information.	Specify the Netstat option VIPADCFG/-F.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

Table 78. Sysplex Distributor - Migration tasks (continued)

Task	Procedure	Reference
Verify workload distribution.	Specify the Netstat options VCRT/-V and VDPT/-O.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Display sysplex-wide Dynamic VIPAs status.	Specify the DISPLAY TCPIP,,SYSPLEX,VIPADYN.	<i>z/OS Communications Server: IP Configuration Reference</i>

Non-disruptive VIPA takeover

The dynamic VIPA support in CS for OS/390 V2R8 allowed a backup stack to takeover the VIPA in cases where the primary stack experienced a system outage. It did not, however, allow non-disruptive movement of the VIPA during normal operations; therefore, there was not a way to preserve existing connections while relocating an application using the VIPA with BIND or IOCTL DVIPA or while recovering the VIPA ownership at the primary stack following an outage. The non-disruptive VIPA takeover function allows for this freedom of movement by maintaining the active connections that were established with the backup (or the prior-owning, in the case of IOCTL or BIND) stack and allowing the VIPA to move immediately back to the primary (or to the new-owning, in the case of IOCTL or BIND) stack. The primary or new-owning stack will then be allowed to accept all new connections requests and will be able to forward the IP datagrams to the backup or prior-owning stack for connections which were active at the time of the non-disruptive takeover. This ensures minimal impact for planned or unplanned system outages since workload can be redirected without affecting existing connections.

Refer to the discussion on Virtual IP Addressing in *z/OS Communications Server: IP Configuration Guide* for complete information.

Restrictions

All participating stacks must be running CS for OS/390 V2R10.

What this change affects

- Customization
- Operation
- Availability

Migration procedures

The non-disruptive VIPA takeover function is *automatically enabled* (it is the default behavior) in CS for OS/390 V2R10 if you have configured VIPADEFINE and VIPARANGE statements. This means that in CS for OS/390 V2R10, VIPADEFINE is automatically set to MOVEABLE IMMEDIATE and VIPARANGE is automatically set to MOVEABLE NONDISRUPTIVE. If you do *not* want non-disruptive VIPA movement, perform the task in the following table.

Table 79. Non-disruptive VIPA takeover - Migration task to prevent enabling of the function

Task	Procedure	Reference
Prevent non-disruptive VIPA takeover.	<ul style="list-style-type: none"> Specify MOVEABLE WHENIDLE on the VIPADEFINE statement when restoring the original stack after a backup stack has activated the DVIPA. Specify MOVEABLE DISRUPTIVE on the VIPARANGE statement for the application-created DVIPAs (the DVIPAs created by IOCTL or BIND). 	z/OS Communications Server: IP Configuration Reference

When using the non-disruptive VIPA takeover function, you may want to perform the tasks in the following table.

Table 80. Non-disruptive VIPA takeover - Optional migration tasks

Task	Procedure	Reference
Display configuration information.	Specify the Netstat option VIPADCFG/-F.	z/OS Communications Server: IP System Administrator's Commands
Display Sysplex-wide Dynamic VIPAs status.	Specify the DISPLAY TCPIP,,SYSPLEX,VIPADYN.	z/OS Communications Server: IP Configuration Reference

Policy-based network function enhancements

Policy Agent enhancements

The z/OS UNIX Policy Agent was introduced in CS for OS/390 V2R7. In CS for OS/390 V2R10, it is enhanced with new functions in the following categories:

- Support for the latest version of the Lightweight Directory Access Protocol (LDAP) policy definitions, known as the *schema*. This version of the schema provides enhanced functionality for grouping policy definitions and specifying their conditions for activation, actions to be performed, and time periods during which they are active.

A subset of the new functionality available with the latest schema is also provided for policies defined in the Policy Agent configuration file. Policies defined using the syntax available with previous releases are known as *Version 1 policies*, while policies defined using the latest schema (or equivalent configuration file support) are known as *Version 2 policies*.

The SLA subagent is changed to support the Version 2 schema. Some of the existing MIB tables are deprecated, and new MIB tables are introduced. This is necessary due to the table indexing changes required by the Version 2 schema.

- Support for enhanced traffic filtering. Policies can now be defined for applications based on the application name and/or application data. This is useful for applications where other information, such as port, is not predictable. From a policy perspective, application data is an arbitrary string of characters, but is currently implemented as a URI string for Web servers using the Fast Response Cache Accelerator (FRCA) function.
- Support for Sysplex Distributor functions. The Policy Agent supports Sysplex Distributor in two ways:
 - Policies can be established that limit the set of target stacks to be considered by Sysplex Distributor for a given set of traffic (for example, a set of clients).
 - The Policy Agent collects policy performance data from target stacks, and derives a QoS weight fraction for each target application in the sysplex. This

weight fraction is used to reduce the Workload Manager (WLM) weight for each target stack. This allows Sysplex Distributor to balance work based on QoS performance data in addition to WLM criteria.

- Support for Traffic Regulation Management (TRM) functions. The Policy Agent can be used to define TR policies for use by the TRM daemon.
- LDAP server support for an an SSL connection, backup server support, server redirection support (where an LDAP query is redirected to another server for processing), and support for both Versions 2 and 3 of LDAP.
- Usability enhancements, including operator messages, STOP command support, and logging to syslog daemon. A new z/OS UNIX command, pasearch, displays policy definitions in greater detail and with a greater degree of filtering than was previously available using the netstat command.

Restrictions

The following restriction applies:

- Policy Agent log files cannot be named SYSLOGD in the current directory. The name SYSLOGD is reserved to indicate logging to the syslog daemon.

Incompatibilities

The following incompatibilities apply:

- The NETSTAT SLAP/onetstat -j command no longer displays policy definition information for defined service policies. Instead, it only displays policy performance information. Use the new pasearch command to display policy definition information.
- The Object IDs (OIDs) for some of the MIB objects supported by the SLA subagent have changed. Refer to the /usr/lpp/tcpip/samples/slapm.txt file for details on the new MIB objects. See Table 166 on page 236 for information about the SLA subagent MIB objects.
- The PolicyName attribute, when used in combination with the PolicyRulesName or PolicyRuleName attribute in defined LDAP server service policies, or when used on the ServicePolicyRules or PolicyRule configuration statement, is no longer supported (it is ignored).
- With the new version of the Policy Agent schema, the default for PolicyScope has changed from DataTraffic to Both.
- *direction* is now implicit in the schema. Also, in the schema for previous releases (Version 1), *source* was defined as local, while *destination* implied remote. With CS for OS/390 V2R10's (Version 2's) schema, source and destination are the actual source and destination.

Refer to *z/OS Communications Server: IP Configuration Reference* for complete information on Version 1 to Version 2 policy changes.

- The Policy Agent now requires superuser authority to be started.
- The Policy Agent -d startup option now requires a numeric value to be supplied as the debug level.

What this change affects

- Customization
- Diagnosis
- Operation

Migration procedures

If you want to take advantage of the Policy Agent and LDAP enhancements, perform the tasks in the following table.

Table 81. Policy Agent and LDAP enhancements - Migration tasks

Task	Procedure	Reference
Use an SSL-secured connection between the Policy Agent and LDAP server.	Configure the SSL parameters on the ReadFromDirectory configuration statement and install the LDAP server's key into the local keyring file.	<i>z/OS Communications Server: IP Configuration Reference</i>
Specify the LDAP protocol version in use by the LDAP server.	Configure the LDAP_ProtocolVersion parameter on the ReadFromDirectory configuration statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Specify the user ID and password to use when connecting to the LDAP server (previous releases used anonymous login).	Configure the user ID (also known as Distinguished Name for user ID) and password parameters on the ReadFromDirectory configuration statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Use a backup LDAP server.	Configure the backup LDAP server address and port parameters on the ReadFromDirectory configuration statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Control the number and size of Policy Agent log files.	Use the PAGENT_LOG_FILE_CONTROL environment variable when starting the Policy Agent.	<i>z/OS Communications Server: IP Configuration Reference</i>
Use the syslog daemon as the Policy Agent log file.	Either specify the -l parameter or change the PAGENT_LOG_FILE environment variable when starting the Policy Agent.	<i>z/OS Communications Server: IP Configuration Reference</i>
Display configured policies, if desired.	Use the pasearch command.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Use the new application name and/or application data policy filtering functions with the Policy Agent.	Define the parameters in your policy definitions.	<i>z/OS Communications Server: IP Configuration Reference</i>
Use the functions and semantics of the new version of the Policy Agent schema.	Define the policies according to the Version 2 schema and configure the schema version on the ReadFromDirectory configuration statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Monitor QoS performance statistics on Sysplex Distributor target stacks.	Configure the PolicyPerfMonitorForSDR configuration statement on the Sysplex Distributor target stacks.	<i>z/OS Communications Server: IP Configuration Reference</i>
Control the set of Sysplex Distributor target stacks to be considered for traffic matching a policy rule.	Configure the outbound interfaces on the policy action that specifies PolicyScope DataTraffic for a given policy rule.	<i>z/OS Communications Server: IP Configuration Reference</i>
Be aware of updated messages if you have performed automation on message text.	Message text of messages EZZ8216I, EZZ8217I, and EZZ8223I has changed.	<i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>

Service Level Policy Quality of Service (QoS) enhancements

Support for Service Level Policy and Quality of Service (QoS) was provided in CS for OS/390 V2R7 for regulation of IP traffic and for service differentiation. The Service Level Policy was enhanced in CS for OS/390 V2R8. In CS for OS/390 V2R10, Service Level Policy and QoS are further enhanced to allow better control of traffic flow within networks. Specifically, these aspects of Service Level Policy are enhanced in CS for OS/390 V2R10:

- Additional traffic characteristics (such as mean rate, peak rates, and burst sizes) are now considered, in addition to previously supported parameters (such as window sizes and number of connections).

- TCP/IP regulates outbound UDP, TCP, and Enterprise Extender traffic that exceeds the requested QoS.
- The aggregation of multiple flows and connections is regulated, ensuring that the aggregate of connections to a given destination does not exceed the desired traffic profile, and that each connection receives a reasonable amount of traffic.
- Adaptive rate-based (ARB) congestion control is invoked to further regulate Enterprise Extender (EE) traffic.

Restrictions

The following are not regulated:

- RAW traffic
- Traffic not originated in the host with the service level policies (such as routed traffic)
- Inbound traffic

What this change affects

- Performance

Migration procedures

If you wish to take advantage of the Service Level Policy QoS enhancements, perform the tasks in the following table.

Table 82. Service Level Policy Quality of Service (QoS) enhancements - Migration tasks

Task	Procedure	Reference
Use Service Level Policy QoS. Copy the three sample start procedures (PAGENT, RSVPD, and PAGTSNMP) and customize, if necessary.	The start procedures reside in SEZAINST.	<i>z/OS Communications Server: IP Configuration Reference</i>
Start the Policy Agent and/or the RSVP Agent.	Authorize the Policy Agent and/or the RSVP Agent to the appropriate security product profiles.	<i>z/OS Communications Server: IP Configuration Reference</i>
Start the SLA subagent.		<i>z/OS Communications Server: IP Configuration Reference</i>
Rebuild the applications that use RAPI.	Recompile and relink RSVP applications to use the RAPI DLL.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Programmer's Reference</i>
Specify RSVP policies by using PolicyScope RSVP (or PolicyScope Both) on the ServicePolicyRules statement.	Replace RSVP CLTOS and GSTOS statements with defined policies. (Required if you previously used the RSVP CLTOS and/or GSTOS configuration statements.)	<i>z/OS Communications Server: IP Configuration Reference</i>
Control the bandwidth of outbound traffic.	Use the new Policy Agent Diffserv parameters when creating differentiated services policies.	<i>z/OS Communications Server: IP Configuration Reference</i>

Traffic Regulation and Management (TRM)

CS for OS/390 V2R10 introduces Traffic Regulation and Management (TRM) support as a way to regulate the number of TCP connections to any given port, depending on which hosts are connecting. This is accomplished through TRM policy, which is controlled by the Policy Agent based on the Traffic Regulation (TR) policies defined to it. TRM is designed to limit the number of TCP connections of a

host, based on a controlling percentage and upper-limit connections that the customer provides depending on the type of traffic expected.

There are three TRM modes:

Limit Refuses connections that do not meet policy specifications.

Log Simulates Limit mode; it logs connections but does not refuse any. Log mode can be used to assess the effectiveness of a configured Traffic Regulation policy.

Statistics

Gathers information about normal traffic patterns on a port, then suggests a reasonable configuration for the port. Statistics mode is used for determining initial policy definitions.

Restrictions

The following restrictions apply:

- Traffic regulation is performed only on incoming TCP connections.
- Traffic regulation policies must be defined in the policy agent configuration file; they are not supported in the LDAP server.

What this change affects

- Customization

Migration procedures

The TRM function does not require any action unless you wish to regulate TCP connections using the new TRM policies. Any existing policy definitions will continue to function as in previous releases. To enable the TRM function, perform the tasks in the following table.

Table 83. Traffic Regulation and Management function - Migration tasks

Task	Procedure	Reference
Configure TRM policies.	Write TRM policy in Policy Agent configuration file.	<i>z/OS Communications Server: IP Configuration Reference</i>
Start Policy Agent.	Start Policy Agent from the z/OS UNIX shell or a started procedure.	<i>z/OS Communications Server: IP Configuration Reference</i>
Start TRMD (Traffic Regulation Management Daemon).	Observe TRMD initialization messages on console, and run with -d option, if necessary, to identify problem.	<i>z/OS Communications Server: IP Configuration Reference</i>
Analyze and refine TRM policies.	Use the trmdstat command to extract TRM statistics from the syslog output.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

Queued Direct I/O (QDIO) queue management for MPCIPA devices

CS for OS/390 V2R10 implements a form of queue management called Random Early Slowdown (RES) for all MPCIPA devices. RES is designed to immediately relieve congestion on outbound QDIO write priority queues for MPCIPA devices. RES works independently for each of the four write priority queues. Specifically, it reduces the TCP congestion window for TCP connections and reduces the windows used by adaptive rate-based (ARB) congestion control for Enterprise Extender traffic. As the name implies, RES slows the traffic flow from randomly-selected connections after congestion is detected on an outbound QDIO queue.

The VTAM DISPLAY TRL command has also been enhanced to display the current congestion state of the VTAM TRLE for this MPCIPA device. For details on these enhancements, see information on messages IST12211 and IST17571 in *z/OS Communications Server: SNA Messages*.

MPCIPA was introduced in CS for OS/390 V2R7. For information on defining MPCIPA devices, refer to *z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: SNA Network Implementation Guide*.

Restrictions

The following restrictions apply:

- UDP traffic, RAW traffic, and traffic not originated from this host (routed traffic) are not subject to Queued Direct I/O queue management.
- Inbound traffic is not subject to Queued Direct I/O queue management.

What this change affects

- Performance

Migration procedures

There are no migration procedures for the QDIO queue management function. In CS for OS/390 V2R10, it is automatically enabled for all MPCIPA devices.

MPCIPA Queued Direct I/O enhancements for Fast Ethernet and ATM LAN-Emulation

CS for OS/390 V2R10 provides significant enhancements for users of an OSA-Express with Fast Ethernet and ATM LAN-Emulation (LE) capability. Starting in CS for OS/390 V2R7, the Queued Direct I/O interface to the OSA-Express could be used for an OSA-Express with Gigabit Ethernet attachment. In CS for OS/390 V2R10, it can also be used for Fast Ethernet and ATM LAN-Emulation (LE) attachments. This allows users with access to Fast Ethernet and ATM networks to take advantage of the highly optimized data-transfer interface of Queued Direct I/O. Among the advantages of Queued Direct I/O are the IP Assist features of Address Resolution Protocol (ARP) Offload, packet filtering, MAC handling by the OSA-Express, and OSA-Express routing.

In addition, the IP Assist features for Queued Direct I/O have been enhanced in this release to provide ARP information. See “MPCIPA Queued Direct I/O Address Resolution Protocol (ARP) cache enhancements” on page 146 for more detail about this ARP information.

Users of OSA-Express with Fast Ethernet and ATM LE attachments can still define these devices as LCS or MPCOSA devices. Note, however, that when using LCS and MPCOSA devices, all currently defined functions and restrictions still apply for these device types, and support is *not* provided for Queued Direct I/O functions such as optimized data-transfer interface and OSA-Express routing. Therefore, IBM recommends defining devices as MPCIPA when using OSA-Express with Fast Ethernet and ATM LE attachments.

Note: ARP statistics (and ARP cache data) are always available for devices defined as LCS. ARP statistics (and ARP cache data) are not available for devices defined as MPCOSA.

In addition, support remains for ATM users of OSA-Express to run ATM without using LAN Emulation (native ATM, defined with a DEVICE type of ATM). Queued Direct I/O is not available for native ATM.

Restrictions

The following restrictions apply:

- Use of the z/OS CS for all Queued Direct I/O interfaces depends on the availability of the Open Systems Adapter (OSA)-Express feature. This feature is available on S/390 Parallel Enterprise Servers - Generation 5 (G5) and Generation 6 (G6) and on zSeries z800 and z900.
- ATM support with OSA-Express using Queued Direct I/O is limited to LAN Emulation mode. Native ATM support, though supported by OSA-Express, cannot use Queued Direct I/O.

What this change affects

- Performance

Migration procedures

The MPCIPA QDIO enhancements for Fast Ethernet and ATM LAN-Emulation does not require any action unless you want to take advantage of Queued Direct I/O for these adapters. If so, perform the tasks in the following table.

Table 84. MPCIPA QDIO enhancements for Fast Ethernet and ATM LAN-Emulation - Migration tasks

Task	Procedure	Reference
Configure the OSA-Express adapter for Queued Direct I/O mode.	Define the CHPID for the OSA-Express as OSD.	<i>S/390: OSA-Express Customer's Guide and Reference</i>
Define corresponding TRLE.	Define a TRLE to represent the OSA-Express Fast Ethernet adapter. It must include MPCLEVEL of QDIO, PORTNAME, one or more DATAPATH addresses, and one READ and one WRITE address.	<i>z/OS Communications Server: SNA Resource Definition Reference</i>
Define the OSA-Express to TCP/IP as an MPCIPA device.	Define a DEVICE statement of type MPCIPA and a LINK statement of type IPAQENET. Ensure the DEVICE name matches the PORTNAME on the TRLE statement above. Specify PRIROUTER, SECROUTER, or NONROUTER as desired. Note: The DEVICE and LINK statements are defined identically whether being used for Fast Ethernet or ATM LAN-Emulation.	<i>z/OS Communications Server: IP Configuration Reference</i>
Understand how Type of Service (priority queuing) affects OSA-Express for Fast Ethernet or ATM LAN Emulation.	Refer to discussion on ToS settings and priority queuing in "Outbound priorities" section of <i>z/OS Communications Server: SNA Network Implementation Guide</i> .	<i>z/OS Communications Server: SNA Network Implementation Guide</i>
Define OSA-Express device for either static routing or OMPROUTE.	For static routes, either code GATEWAY statements using a next-hop IP address on the Ethernet, or use the BEGINROUTES statement. For OMPROUTE, use OSPF_Interface statements if OSPF is the routing protocol being used or, if RIP is being used, use RIP_Interface statements. Note that Jumbo frames are not supported for Fast Ethernet or ATM LAN-Emulation, and the MTU size is 1492.	<i>z/OS Communications Server: IP Configuration Reference</i>

MPCIPA Queued Direct I/O Address Resolution Protocol (ARP) cache enhancements

This enhancement provides the retrieval of ARP information by TCP/IP for those devices which perform an ARP offload function (those devices which maintain the ARP information in the device adapter) and which support the retrieval of the ARP information by TCP/IP. In particular, ARP cache data for these devices will be displayed by the existing netstat ARP/-R reports and SNMP queries, and ARP counters will be available by using the existing SIOCGMONDATA ioctl. This data will be available for all users of Queued Direct I/O, including Gigabit Ethernet users, Fast Ethernet users, and ATM LAN-Emulation users, although users of OSA-Express with Gigabit Ethernet capability will require a minimum of OSA-Express microcode level 4.06 to take advantage of this enhancement.

The netstat DEVLINKS/-d report has been updated with new fields for these devices which indicate the status of their ARP offload support. The new ArpOffload field is displayed only if the device is active and performs an ARP offload function. That is, the device performs the ARP caching function and maintains ARP counters instead of the TCP/IP stack performing these functions. The new ArpOffloadInfo field indicates whether the ARP cache data and ARP counters can be retrieved from the device by the TCP/IP stack.

For more information about devices which support the ARP offload function, refer to *z/OS Communications Server: IP Configuration Guide*.

Restrictions

The device must support the Query ARP information interface for retrieval of ARP cache information from the device by TCP/IP. If the OSA-Express adapter is being shared by multiple TCP/IP instances, then the ARP counter data returned by OSA-Express represents usage of the adapter by all TCP/IP instances, not just the TCP/IP instance on which the SIOCGMONDATA ioctl was processed.

What this change affects

- Customization
- Automation
- Diagnosis

Migration procedures

If you want to take advantage of the MPCIPA Queued Direct I/O Address Resolution Protocol (ARP) cache enhancements, perform the task in the following table.

Table 85. MPCIPA QDIO ARP cache enhancements - Migration task

Task	Procedure	Reference
Take advantage of new information on the report.	Change automation to accommodate new fields on netstat DEVLINKS/-d report. Use the Netstat ARP/-R report to display ARP cache data.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

syslogd isolation

With the CS for OS/390 V2R10 syslogd isolation enhancement, additional controls are provided for segregating trace records from different applications. Specifically, the syslogd isolation enhancement provides the following new functions:

- When a new syslogd command-line parameter is specified, the user ID and job name associated with the trace record writer will be stored in the trace record.
- User ID and job name can be used along with existing facility and priority criteria to select trace records.
- When a new syslogd command-line parameter is specified, syslogd will not accept messages received from other hosts.
- Special format strings in file names specified in the syslogd configuration file will be replaced with the current time or date.
- Trace records can be logged to SMF using \$SMF as the destination in the syslogd configuration file.
- Additional configuration file errors are detected.
- When a new syslogd command-line parameter is specified, syslogd will create new log files and directories.

Restrictions

None.

Incompatibilities

The ability for syslogd to substitute the current time or date in file names is incompatible with the existing ability for file names to contain a percent sign (%). File names in the syslogd configuration file that contain a percent sign must be changed to use two percent signs.

What this change affects

- Customization
- Diagnosis

Migration procedures

If you want to take advantage of the syslogd isolation enhancement, perform the tasks in the following table.

Table 86. *syslogd isolation - Migration tasks*

Task	Procedure	Reference
Include the user ID and job name on trace records stored by syslogd.	Add -u to the syslogd command line.	<i>z/OS Communications Server: IP Configuration Guide</i>
Use user ID and job name, in addition to facility and priority, to select trace records.	Change syslogd rules in the syslogd configuration file to use the new syntax userid.jobname.facility.priority instead of facility.priority.	<i>z/OS Communications Server: IP Configuration Guide</i>
Disable the processing of syslog messages received from other hosts.	Add -i to the syslogd command line.	<i>z/OS Communications Server: IP Configuration Guide</i>
Avoid problems with existing trace files that contain percent signs in the file name.	Required; to prevent the percent sign from being interpreted as a format string, replace each percent sign with two percent signs in every file name specified in the syslogd configuration file.	<i>z/OS Communications Server: IP Configuration Guide</i>

Table 86. syslogd isolation - Migration tasks (continued)

Task	Procedure	Reference
Write trace records to files that contain the current time and/or date in the file names.	Edit the file names specified in the syslogd configuration file to contain strftime() format strings. For example, /log/local1.%Y.%j will be expanded to /log/local1.2001.011 when syslogd is started or restarted on January 11, 2001.	<i>z/OS Communications Server: IP Configuration Guide</i>
If you are using the syslogd provided with OS/390 Security Server, you must migrate to the Communications Server for OS/390 syslogd.	Create a syslogd configuration file and modify the start procedure to run /usr/bin/syslogd instead of the OS/390 Security Server syslogd.	<i>z/OS Communications Server: IP Configuration Guide</i>
Check for and correct any errors.	If you receive configuration file error messages when starting syslogd, consult the User Response for the message.	<i>z/OS UNIX System Services Messages and Codes</i>
Optionally, create missing syslogd log files and directories automatically.	Add -c to the syslogd command line.	<i>z/OS Communications Server: IP Configuration Guide</i>
Optionally, send your log to SMF (record type 109).	Indicate \$SMF as the destination in the syslogd configuration file.	<i>z/OS Communications Server: IP Configuration Guide</i>

Access control for ports, stack, and network

Port access control

Port access control is a CS for OS/390 V2R10 system security enhancement to the PORT and PORTRANGE statements to protect against unauthorized use of ports. It allows control of an application's ability to bind to specific TCP and UDP ports or port ranges using a security product, such as the z/OS security server (RACF). This enhancement is provided by the SAF keyword on the PORT or PORTRANGE statement in the TCP/IP profile or by using OBEYFILE.

PORT or PORTRANGE may be reserved with the wildcard user name *. The use of * along with SAF allows the PORT or PORTRANGE to be made available to any user who is permitted to the SAF resource. The user name of RESERVED prevents the use of the ports indicated by PORT or PORTRANGE.

The following applications are now APF-authorized and are usable when TCPCONFIG RESTRICTLOWPORTS is specified:

- LPR - print a file
- LPRM - remove a print job
- LPQ - query print jobs
- RSH - Remote Shell Client

Note: In order for these commands to actually run in authorized state, they must be listed in IKJTSOxx using the AUTHCMD NAMES statement.

All CS for OS/390 V2R10 installations are encouraged to use both TCPCONFIG RESTRICTLOWPORTS and UDPCONFIG RESTRICTLOWPORTS to enhance system security by preventing unintended use of well-known ports.

Note: If SAF resources are defined on PORT or PORTRANGE statements, this information will appear on the D TCPIP,,NETSTAT,PORTL command output only. There is no change to the netstat or onetstat output under TSO or the z/OS UNIX shell for this function.

Refer to the EZARACF sample in SEZAINST or *z/OS Communications Server: IP Configuration Reference* for details on the format of the complete RACF profile name.

Restrictions

A security product that supports the SERVAUTH class, such as z/OS security server (RACF), is required to use the SAF keyword. The SERVAUTH class must be RACLISTed and the user IDs that clients or servers run under must be permitted to the resource name that protects the port.

What this change affects

- Customization
- Installation
- Operation

Migration procedures

If you want to take advantage of the port access control enhancement, perform the tasks in the following table.

Table 87. Port access control - Migration tasks

Task	Procedure	Reference
Configure security product definitions.	Ensure that a security product that supports the SERVAUTH class is installed prior to using the SAF keyword. Also ensure that the SERVAUTH class is RACLISTed.	<i>z/OS Communications Server: IP Configuration Reference</i>
Authorize user IDs for clients and servers for port access control.	For each stack that has a port access resource defined to the security product, you must permit user IDs for clients or servers that use the port.	<i>z/OS Communications Server: IP Configuration Reference</i>
Protect port and portranges.	Use the SAF keyword on the PORT or PORTRANGE statement to specify an SAF resource name. This specifies only the rightmost qualifier of the complete resource name. If the SAF keyword is not coded, there is no change in function from previous releases.	<i>z/OS Communications Server: IP Configuration Reference</i>
Use the newly APF-authorized clients from TSO.	Update the IKJTSOxx PARMLIB member to list these as authorized commands.	For information on updating parmlib, refer to <i>z/OS MVS Initialization and Tuning Reference</i> . For information on using the clients, refer to <i>z/OS Communications Server: IP Configuration Guide</i> .

Stack access control

Stack access control is a CS for OS/390 V2R10 function that allows control of access to the TCP/IP stack using a security product, such as the z/OS security server (RACF). This allows you a way to prevent unauthorized users from using the TCP/IP stack by way of a TCP, UDP, or RAW socket. This function is provided by a

new Security Access Facility (SAF) resource in the SERVAUTH class. Stack access control is not applicable to TCP/IP releases prior to CS for OS/390 V2R10.

Refer to the EZARACF sample in SEZAINST for details on the format of the complete RACF profile name.

Restrictions

To use the stack access control function, the SAF resource must be defined to the security product in the SERVAUTH class. The SERVAUTH class must be RACLISTed.

What this change affects

- Customization
- Installation
- Operation
- System Security

Migration procedures

If you want to take advantage of the stack access control function, perform the tasks in the following table.

Table 88. Stack access control - Migration tasks

Task	Procedure	Reference
Configure security product for stack access control.	Define a SAF resource in the SERVAUTH class for each TCP/IP stack. The SERVAUTH class must be RACLISTed. If the stack access control SAF resource is not defined to RACF, no stack access checking will be in effect. Non-IBM security products may require the stack access resource to be defined and users be permitted to the resource in order to access the stack. If you use multiple stacks, each stack should have its own SAF resource defined for stack access control.	<i>z/OS Communications Server: IP Configuration Guide</i>
Authorize users to the stack access resource.	For each stack that has a stack access resource defined to the security product, you must permit users or groups to the resource. Non-permitted users will not be able to run any program or utility that requires access to the TCP/IP stack.	<i>z/OS Communications Server: IP Configuration Guide</i>

Network access control

CS for OS/390 V2R10 provides a new network access control function to enable system administrators to assign permission for users to access certain networks and resources; therefore, they can disallow the ability of certain users to send data from z/OS to certain networks. System administrators can now classify IP networks into security zones in which a network is defined to have a certain level of security sensitivity based on its security zone. Just as all hosts and interfaces can belong to multiple networks, hosts and interfaces can belong to multiple security zones.

Since this function restricts a user's ability to communicate with certain networks, certain user IDs (such as those associated with common servers) should be included on all resource access lists to ensure they function properly. Examples of common servers include FTP and Web Servers. In addition, it is recommended that all users are allowed the ability to communicate with the domain name server which they use.

Refer to the EZARACF sample in SEZAINST or *z/OS Communications Server: IP Configuration Reference* for details on the format of the complete RACF profile name.

Note: If network access entries are defined to TCP/IP, this information will appear on D TCPIP,,NETSTAT,ACCESS,NETWORK command output only. There is no change to the netstat or onetstat output under TSO or the z/OS UNIX shell for this function.

Restrictions

A security product that supports the SERVAUTH class, such as z/OS security server (RACF), is required for use of this function. The SERVAUTH class must be RACLISTed and the user IDs that clients or servers run under must be permitted to the resource names that protect each network.

What this change affects

- Customization
- Installation
- Operation
- Diagnosis
- System Security

Migration procedures

If you want to take advantage of the network access control function, perform the tasks in the following table. No TCP/IP configuration reference changes are required if this new function will *not* be used in your installation.

Table 89. Network access control- Migration tasks

Task	Procedure	Reference
Configure the security product for network access control.	Define SAF resources in the SERVAUTH class. The SERVAUTH class must be RACLISTed. Permit users or groups READ access to the resource or resources.	<i>z/OS Communications Server: IP Configuration Guide</i>
Use the new network access control function to restrict user access to networks or hosts.	Include network access statements (NETACCESS/ENDNETACCESS) in a TCPIP profile or OBEYFILE.	<i>z/OS Communications Server: IP Configuration Reference</i>

Server bind control

Server bind control is new for CS for OS/390 V2R10 and it allows specification of an interface or VIPA address for a generic server to bind to instead of INADDR_ANY. This function allows multiple servers to bind to the same port on different interfaces. For example, this function would allow the Telnet 3270 server and the z/OS UNIX Telnet server to both listen on port 23.

Restrictions

The following restrictions apply:

- The BIND keyword followed by a dotted decimal IP address is valid on the PORT statement when reserving TCP or UDP ports. It is not valid for PORTRANGE.
- A server should not be dependent on the value returned by the getsockname() socket call.

What this change affects

- Customization

Migration procedures

If you want to take advantage of the server bind control function, perform the tasks in the following table.

Table 90. Server bind control - Migration tasks

Task	Procedure	Reference
Define a PORT statement for each application that now binds to INADDR_ANY but that needs to be restricted to a single IP address.	The user name on each port statement should be the unique jobname of the server (or the TSO user ID if the server is run under TSO).	<i>z/OS Communications Server: IP Configuration Reference</i>
Assign a unique interface address or VIPA address for each server that will share a port.	Code the BIND ipaddr keyword on the PORT statement. BIND causes INADDR_ANY binds to the specified port to be converted into specific binds for the specified address (which can include static or dynamic VIPA addresses).	<i>z/OS Communications Server: IP Configuration Reference</i>
Select the server to be used in communications.	Clients should specify the correct target IP address or DNS name for each server.	<i>z/OS Communications Server: IP Configuration Reference</i>

On-demand tunnels

CS for OS/390 V2R10 enhances the Internet Key Exchange (IKE) function that was introduced in CS for OS/390 V2R8. In CS for OS/390 V2R8, dynamic tunnels had to be started manually before any traffic could flow across the tunnel. With the on-demand tunnels enhancement, the flow of data starts a negotiation, thus alleviating the need to start it manually.

When a tunnel is being negotiated, all packets (data) that are tunnel bound are discarded. The applications must retransmit the packets for successful delivery. For a local TCP client, the transport layer (TCP) will be signaled once the tunnel is established. This will transmit the unacknowledged packets immediately.

Restrictions

None.

What this change affects

- Security
- Usability

Migration procedures

Configuration for on-demand tunnels is performed when setting up the z/OS security server.

REXEC enhancements

The Remote Execution Server for TSO commands was enhanced in this release with the ability to control the job name prefix of batch jobs submitted by the server, and also to remove a length restriction on the accounting field of the job card of jobs modified by the optional user exit. Additionally, job output of jobs submitted by the server can optionally be prevented from being automatically purged, thus aiding in debugging the optional user exit.

The length of job option parameter names may not exceed 100 characters; therefore, abbreviations of option parameter names are allowed. Refer to *z/OS Communications Server: IP Configuration Reference* for the valid abbreviations.

Restrictions

None.

What this change affects

- Customization
- Diagnosis
- Operations
- Security

Migration procedures

If you want to take advantage of the REXEC enhancements function, perform the tasks in the following table.

Table 91. REXEC - Migration tasks

Task	Procedure	Reference
Control prefix of job names submitted by the server.	Specify the PREFIX parm on the Remote Execution Cataloged Procedure.	<i>z/OS Communications Server: IP Configuration Reference</i>
Exploit longer accounting fields on the JOB card of jobs submitted by the server.	Modify the optional user exit to supply longer accounting fields on the JOB card.	<i>z/OS Communications Server: IP Configuration Reference</i>
Debug errors in the optional user exit by observing the failed job output of jobs submitted by the server.	Specify PURGE parm with a value of N on the Remote Execution Cataloged Procedure, or by using the MODIFY command.	<i>z/OS Communications Server: IP Configuration Reference</i>
Optionally update or enhance any automated tasks keying off system console messages.	Review the new or changed messages affected by this functional enhancement in this release.	<i>z/OS Communications Server: IP Messages Volume 1 (EZA) and z/OS Communications Server: IP Messages Volume 2 (EZB) and z/OS Communications Server: IP Messages Volume 3 (EZY)</i>

IPv6 API

IPv6 API support is added in CS for OS/390 V2R10 for applications that use the Language Environment C/C++ API and z/OS UNIX Assembler Callable Services API. This support, particularly with respect to the support for the C/C++ API, enables applications written to use AF_INET6 socket addresses to operate on z/OS.

Restrictions

Note: The following restrictions are true for CS for OS/390 V2R10 and are included here for reference purposes. Note, however, that they have been removed in z/OS CS V1R4. See “IPv6 support for socket API commands” on page 87 for the updates of z/OS CS V1R4.

Supported IPv6 address formats are IPv4-mapped IPv6 addresses, IN6ADDR_LOOPBACK, and IN6ADDR_ANY. Other IPv6 address formats are not supported.

This function is not supported in a Common INET environment.

What this change affects

- Application Development

Migration procedures

If you want to take advantage of the IPv6 API support, perform the tasks in the following table.

Table 92. IPv6 API - Migration tasks

Task	Procedure	Reference
Enable AF_INET6 support in the system.	Code an AF_INET6 NETWORK statement in the BPX parmlib member.	<i>z/OS UNIX System Services Planning</i>
Use AF_INET6 socket addresses.	Modify application program source code.	RFC 2553

High Speed Access Services (HSAS)

Support for the High Speed Access Services (HSAS) is discontinued in CS for OS/390 V2R10. Use the z/OS TCP/IP stack instead.

Restrictions

None.

What this change affects

- Customization

Migration procedures

If you were previously using HSAS or High Speed Web Access (HSWA), perform the tasks in the following table.

Table 93. High Speed Access Services - Migration tasks

Task	Procedure	Reference
Update the BPXPRMxx parmlib member.	Remove the SUBFILESYSTYPE statement for OESTACK.	None.

Table 93. High Speed Access Services - Migration tasks (continued)

Task	Procedure	Reference
Update any z/OS UNIX shell scripts	Remove any invocations of the following commands: <ul style="list-style-type: none"> • oeifconfig • oeroute • oeping • oenetstat • oenetopts 	None.
Update the application or ENV file if necessary.	If you have any application which explicitly establishes affinity to the name "OESTACK" by one of the following means: <ul style="list-style-type: none"> • the setibmopt() socket call • the SIOCSETRTTD IOCTL • the z/OS UNIX System Services environment variable (ENV) <code>_BPXK_SETIBMOPT_TRANSPORT</code> or <code>_BPXK_INET_FASTPATH</code> (either by way of the <code>setenv()</code> call or in an ENV file) then update the application or ENV file to either specify the appropriate TCP/IP stack name or to remove the request for stack affinity altogether.	<i>z/OS Communications Server: IP Application Programming Interface Guide</i>

Express Logon feature: Digital Certificate Access Server (DCAS)

Express Logon is a new feature in CS for OS/390 V2R10 that allows a user on a workstation, with a TN3270 client and an X.509 certificate, to log on to an SNA application *without* entering an ID or password. This function is initially intended for use by organizations using IBM TN3270 servers that do not reside on the System/390®, such as IBM's CS/2, CS/NT, or CS/AIX. These servers are referred to as *middle-tier* TN3270 servers.

IBM products currently supporting Express Logon are the following:

- TN3270 client:
 - Host On-Demand V5.0

IBM TN3270 middle-tier servers:

- CS/2 6.1
- CS/NT 6.1.1 PTF
- CS/AIX 6.0.0.1 PTF

For more information about Express Logon, refer to *z/OS Communications Server: IP Configuration Reference*, *z/OS Communications Server: IP Configuration Guide*, and *z/OS Communications Server: IP Diagnosis*.

Restrictions

There are no restrictions for using the Express Logon feature.

What This Change Affects

The Express Logon feature affects customization.

Migration procedures

If you want to take advantage of Express Logon feature and the DCAS, perform the tasks in the following table.

Table 94. Express Logon feature: DCAS - Migration tasks

Task	Procedure	Reference
Set up the DCAS to use System SSL with client authentication. Create certificates and keyrings.	<ul style="list-style-type: none"> • Create a keyring and X.509 certificate. You can use gskkyman tool. • Transfer the middle-tier TN3270 server certificate to the host and store in the DCAS keyring. • Transfer the DCAS certificate to the middle-tier system and store in the keyring. 	<i>z/OS Communications Server: IP Configuration Reference and z/OS Communications Server: IP Configuration Guide</i>
Configure the DCAS: <ol style="list-style-type: none"> 1. Configure the DCAS to listen on a port. 2. Ensure the SSL keyring is defined in the HFS or in RACF. 3. Determine the level of client authentication to be used by the DCAS. 4. Determine the level of cipher that SSL will use. 	Create a DCAS configuration file: <ul style="list-style-type: none"> • Use the IPADDR and PORT keywords. • Use the KEYPING and STASHFILE or SAFKEYRING configuration keywords to point the DCAS to the keyring. • Use the CLIENTAUTH keyword to configure the level of client authentication desired. • Use the V3CIPHER keyword. If you do not specify V3CIPHER, the cipher level defaults to the level provided by SSL on your system. 	<i>z/OS Communications Server: IP Configuration Reference and z/OS Communications Server: IP Configuration Guide</i>

Table 94. Express Logon feature: DCAS - Migration tasks (continued)

<p>Set up the DCAS to use RACF services:</p> <ol style="list-style-type: none"> 1. Permit the DCAS to use RACF certificate services. 2. Define the digital certificate of the workstation end user to RACF. 3. Define a PTKTDATA (PassTicket data) profile in RACF where the application name portion matches the application ID entered by the workstation end user. 4. If CLIENTAUTH LOCAL2 is configured, define the certificate used by the middle-tier TN3270 server in RACF to be associated with a user ID. This user ID could be the user ID associated with the running DCAS or any other valid user ID. 	<ul style="list-style-type: none"> • Use the following commands to permit the DCAS to use RACF certificate services: <ul style="list-style-type: none"> – SETROPTS CLASSACT(DIGTCERT DIGTRING) – RDEFINE FACILITY (IRR.DIGTCERT.function) UACC(NONE) – PERMIT IRR.DIGTCERT.function • Define a digital certificate by using the RACDCERT ID() ADD() TRUST command. • Define the PassTicket profile for the application that the end user will log on to using RDEFINE PTKTDATA <i>profilename</i> SSIGNON. Understand how RACF determines the profile name for the type of application you are using. Define a certificate used by the middle-tier TN3270 server in RACF by using RACDCERT ID() ADD() TRUST command. <p>Note: If using RACF to create keyrings, use the following RACF commands:</p> <ul style="list-style-type: none"> • RACDCERT ADDRING • RACDCERT GENCERT • RACDCERT CONNECT • RACDCERT EXPORT 	<p><i>z/OS Communications Server: IP Configuration Reference and z/OS Communications Server: IP Configuration Guide</i></p>
<p>Start the DCAS.</p>	<p>Use one of the following:</p> <ul style="list-style-type: none"> • MVS started procedure • UNIX shell start command • Autolog statement (for automatic start) 	<p><i>z/OS Communications Server: IP Configuration Reference and z/OS Communications Server: IP Configuration Guide</i></p>

Table 94. Express Logon feature: DCAS - Migration tasks (continued)

Use RACF APAR if necessary.	RACF APAR OW44393 is required when using the following: <ul style="list-style-type: none"> • TSO with Generic Resources and PTKDATA Class profiles. • Applications with shared user IDs that could access the application simultaneously. RACF requires the PTKDATA profile to specify APPLDATA('NO REPLAY PROTECTION.') 	APAR OW44393
Diagnose Express Logon problems, if necessary.	Follow the appropriate instructions.	<i>z/OS Communications Server: IP Diagnosis</i>

Serviceability enhancements

TCP/IP IPCS command enhancements

The TCP/IP IPCS commands are improved in CS for OS/390 V2R10. The commands execute faster and their syntax is more consistent. Specifically, CS for OS/390 V2R10 introduces the following enhancements to the IPCS commands:

- The syntax has changed for all TCPIPCS commands with variable parameters. Now, all variable parameters must be listed first; if more than one is specified, they must be in an extra set of parentheses. If no variable parameters are needed but keywords are needed, an asterisk (*) must be used in place of the variable parameters.
- The following TCPIPCS commands now have SUMMARY as the default and DETAIL is an option: CONFIG, LOCK, PROTOCOL, RAW, SOCKET, STREAM, TCB, TELNET, TIMER, TRACE, TREE, and UDP. Formerly, some of these commands had SUMMARY, ALL, or FORM as an option.
- TCPIPCS HELP is now documented and is more complete.
- TCPIPCS MTABLE now allows a module name as input.
- TCPIPCS PROFILE no longer has the option of creating a data set (IPCSPRNT can be used to save the output).
- TCPIPCS PROTOCOL no longer has the control block address option. Note that PROTOCOL invokes RAW, TCB, and UDP, which can be invoked with a CB address.
- TCPIPCS STORAGE no longer has control block parameters. All storage is summarized.
- TCPIPCS STREAM now has the SKSH options.
- TCPIPCS TRACE options have changed. Now, only SUMMARY and DETAIL are provided. The output has been shortened.
- TCPIPCS TREE options have changed. Duplicate ones have been deleted and new ones added, and BOTH is now the default.
- The REXX run-time library is no longer used.
- Fewer IPCS symbols are now set. Only 9 are now set: TSEBPTR, TSEB1, TSEB2, ..., TSEB8

Refer to *z/OS Communications Server: IP Diagnosis* for details on all commands. See “IPCS subcommands” on page 61 for more information about IPCS commands.

Restrictions

None.

Incompatibilities

Command syntax has changed for some commands. The INETSTAT and TCPIP CS SKSH commands were deleted. The following commands were added:

- TCPIP CS API
- TCPIP CS CONNECTION
- TCPIP CS FIREWALL
- TCPIP CS FRCA
- TCPIP CS HASH
- TCPIP CS POLICY
- TCPIP CS VMCF
- TCPIP CS XCF

What this change affects

- Diagnosis

Migration procedures

If you want to take advantage of the TCP/IP IPCS command enhancements, perform the tasks in the following table.

Table 95. TCP/IP IPCS command enhancements - Migration tasks

Task	Procedure	Reference
Use the TCPIP CS commands.	Set up the data set concatenations. (The concatenations changed in CS for OS/390 V2R10.)	<i>z/OS Communications Server: IP Diagnosis</i> , chapter on TCPIP CS
Do not use the TCPIP CS SKSH command.	Use the TCPIP CS STREAM command, which now includes the former TCPIP CS SKSH function.	<i>z/OS Communications Server: IP Diagnosis</i> , chapter on TCPIP CS

Socket API trace

CS for OS/390 V2R10 includes new component trace records to aid application programmers using the TCP/IP Macro API or Callable API to diagnose problems in their applications. These trace records are in the SYSTCPIP trace component under a new option, SOCKAPI.

Furthermore, the Macro API and CALL Instruction API now fully support the SO_SNDBUF and SO_RCVBUF options for the GETSOCKOPT and SETSOCKOPT calls.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

If you want to take advantage of the Socket API trace function, perform the tasks in the following table.

Table 96. Socket API trace - Migration tasks

Task	Procedure	Reference
Use new trace option for socket APIs.	Specify the SOCKAPI option (or ALL options) for Ctrace component SYSTCPIP.	<i>z/OS Communications Server: IP Diagnosis</i>
Use new options on API calls.	Modify application program source code.	<i>z/OS Communications Server: IP Application Programming Interface Guide</i>

TCP/IP trace enhancements

CS for OS/390 V2R10 includes several enhancements to improve diagnosis for TCP/IP:

- A new option is introduced to display module prefix information (compile date, and so on) for most TCP/IP stack, PFS layer, and Telnet modules.
- Group names for the component trace allow you to specify several options with one option.
- Some component trace options have been merged to minimize the number of options.
- Component trace formatting has been improved to make it easier to find failure cases and to see the state of some key data fields.
- The maximum buffer size for the TCP/IP component trace (for example, the size of the component trace dataspace TCPIPDS1) has been increased from 16M to 256M.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

If you want to take advantage of the TCP/IP trace enhancements, perform the tasks in the following table.

Table 97. TCP/IP trace enhancements - Migration tasks

Task	Procedure	Reference
Use the larger buffer size.	Change the component trace option data set.	<i>z/OS Communications Server: IP Diagnosis</i>
Instead of using the AMBLIST to calculate the address of a module for a SLIP trap, use the new DISPLAY TCPIP,,STOR,MODULE command.	Issue the console command DISPLAY TCPIP,,STOR,MODULE=module_name for the TCP/IP module whose location is needed.	<i>z/OS Communications Server: IP Configuration Reference</i>

Performance improvements

Fast Local Sockets

Fast Local Sockets is a new feature in CS for OS/390 V2R10 that provides a performance improvement when both the source and destination of a packet are known to and managed by a single TCP/IP stack. Performance is enhanced when

applications residing on the same MVS image and communicating through the same TCP/IP use a home address instead of a loopback address (for example 127.0.0.1) when sending data.

Restrictions

The following types of non-loopback addresses in the HOME list are not candidates to take advantage of Fast Local Sockets: broadcast, multicast, distributing dynamic VIPAs (VIPADISTribute), or dynamic DVIPAs defined as MOVEable IMMEDIATE or MOVEable NONDISRUPTive.

What this change affects

- Customization — sockets application programming
- Performance

Migration procedures

If you want to take advantage of the Fast Local Sockets enhancement, perform the tasks in the following table.

Table 98. Fast Local Sockets - Migration tasks

Task	Procedure	Reference
Use a home address instead of the traditional loopback address.	<p>Configure your sockets application to use a home address in the SOCKADDR passed on socket calls like BIND, CONNECT, and SENDTO, or else invoke applications with different parameters. Use the output in the address field of the sockaddr passed on subsequent bind(), connect() and sendto() socket calls.</p> <p>The following are some examples of when a non-loopback home address can be used instead of a loopback address:</p> <ul style="list-style-type: none"> • NSINTERADDR in TCPIP.DATA (note, in z/OS CS V1R2, NAMESERVER is also available to specify an address in TCPIP.DATA.) • osnmp configuration • DDNS Server configuration • DNS Forward Domain Data File • Resolver Configuration File - onslookup • SNMPD.CONF 	<i>z/OS Communications Server: IP Application Programming Interface Guide</i>
Change the application code for performance enhancement.	Issue the gethostid() call rather than hardcoding 127.0.0.1 and save the result.	<i>z/OS Communications Server: IP Application Programming Interface Guide</i>

Fast Response Cache Accelerator (FRCA) enhancement

CS for OS/390 V2R7 used Fast Response Cache Accelerator (FRCA) to speed up the processing of static web pages by the WebSphere® Application Server. CS for OS/390 V2R10 provides an enhancement so that the cache serving responsibility can be passed back from the WebSphere application to the TCP/IP stack Fast Response Cache Accelerator. This results in faster response time for the web client if the web content includes dynamic web pages.

Restrictions

To use the Cache Accelerator and control resource consumption (for example, CPU usage), the WebSphere Application Server must have access to Workload Manager (WLM) services or superuser authority. No other RACF check is required.

Notes:

1. The Cache Accelerator is configured on a "per listening socket" basis.
2. WLM support for requests is limited to one enclave per listening socket.

What this change affects

- Performance

Migration procedures

Fast Response Cache Accelerator does not require any action. Implementation requires the following:

1. Configure through the WebSphere Application Server. Refer to the WebSphere Application Server online documentation at <http://www.software.ibm.com/webervers/appserv/>.
2. Use the new NETSTAT CACHINFO and onetstat -C options to display information about the Cache Accelerator. For details, refer to *z/OS Communications Server: IP System Administrator's Commands*.
3. Be aware of the new RACF facility class, BPX.SOCKET.CACHE, that has been added to support Cache Accelerator. The new RACF facility class is only required when using Cache Accelerator with WLM feature. For details, refer to *z/OS UNIX System Services Planning*.

No additional tasks are required to take advantage of the FRCA and web responsibility passing function.

IP Security (IPSec)

CS for OS/390 V2R10 enhances IP Security to increase the throughput and performance for both IPSec and non-IPSec traffic.

Restrictions

None.

What this change affects

- Performance

Migration procedures

There are no z/OS CS tasks for the IP Security enhancement. Refer to *z/OS Security Server Firewall Technologies* for information on the z/OS firewall.

Route lookup improvements

CS for OS/390 V2R10 includes significant performance enhancements to IP routing:

- Route lookup is optimized to reduce mainframe cycle consumption and boost throughput for routing-intensive functions (for example, IP Forwarding).
- Management of the IP routing table is enhanced, thus allowing high data rates (and low storage consumption) to be sustained during heavy bursts of dynamic routing updates.
- Netstat route and gateway display performance are improved in the following ways:
 - Netstat ROUTE/-r and GATE/-g displays are enhanced to include routes for each HOME list IP address and routes dynamically created as part of Path MTU Discovery support. Prior to CS for OS/390 V2R10, the routes existed but were filtered out and not displayed.
 - The restriction on using the TRACERTE/otracert command with the loopback address is removed.

- The TCP/IP stack now supports all classes of IP addresses.

CS for OS/390 V2R10 also introduces a new component trace option, ROUTE, which is used in diagnosis.

Restrictions

None.

Incompatibilities

The CTC trace option is no longer supported.

What this change affects

- Performance
- Diagnosis

Migration procedures

No configuration changes are necessary for route lookup improvements. The tasks in the following table are optional.

Table 99. Route lookup improvements - Migration tasks

Task	Procedure	Reference
Modify the automation for route displays, if necessary.	If the user automation is impacted by the additional routes or the route type changes, then automation will have to be modified.	<i>z/OS Communications Server: IP Configuration Reference</i>
Turn on component tracing to aid in diagnosis.	Add the ROUTE option to the trace command.	<i>z/OS Communications Server: IP Diagnosis</i>

CDLC device driver support for greater than 4K MTU

In releases prior to CS for OS/390 V2R10, the device driver for 3745/46 channel DLC (CDLC) devices was limited to buffer size of less than or equal to 4096 bytes. In CS for OS/390 V2R10, this restriction is relaxed to allow for specification of CDLC Buffer Sizes of up to 8192 and IP CDLC MTU of up to 7167 bytes.

If you are using the CDLC protocol to communicate between the mainframe and 3746, and using 3746 TIC3 adapters (for Token-Ring access), or using ATM (by using the MAE), you may wish to adjust your CDLC device and routing statements to increase the channel frame size and IP MTU carried across the channel. This will provide a throughput improvement, along with CPU reduction, when communicating with a 3746 that supports an MTU larger than 4096 bytes on the LAN or WAN.

Restrictions

None.

What this change affects

- Performance

Migration procedures

If you want to take advantage of the CDLC device driver performance improvement, perform the tasks in the following table.

Table 100. CDLC device driver performance improvement - Migration tasks

Task	Procedure	Reference
Determine whether the configuration would benefit from a larger CDLC buffer size and MTU specification. This new support is intended for configurations in which the 3746 is acting as a router between the mainframe and Token Ring and/or ATM networks.	Verify that the mainframe is communicating to a 3746 IP router that supports and exploits large (>4096-byte) MTUs on either Token Ring or ATM. If so, the configuration would achieve higher throughput by using this enhancement.	Consult your 3746 configuration to determine Token Ring and/or ATM MTUs in effect.
Pick new (larger) IP MTU for the CDLC Link.	Pick an MTU for the CDLC connection that will make better use of both the channel and the large-frame adapters on the network side of the 3746.	
Update TCP/IP to specify larger CDLC channel buffers and MTU.	Within your TCP/IP profile, update the Write_Size and Read_Size parms on the CDLC Device Statement. Also update the MTU or Max_Packet_Size parms on any BeginRoutes, BSDRoutingParms, or GATEWAY entries that are pointing to the CDLC link.	<i>z/OS Communications Server: IP Configuration Reference</i>
Stop and restart TCP/IP.		
Verify the CDLC buffer size and MTU changes now result in large TCP segments end-to-end.	To verify that a TCP-layer connection can now negotiate to the larger Maximum Segment Size (MSS), use a packet trace, or a CCWTRACE, or a Sniffer Trace to verify the IP datagrams are of the new, larger MTU size. (Check the IP_Length field, the halfword at +2 within the IP Header.)	<i>z/OS Communications Server: IP Diagnosis</i>

CLAW packing within a 4K frame

In CS for OS/390 V2R10, CLAW performance is improved for small MTU traffic when CS for OS/390 is communicating with Cisco 7200-series and 7500-series routers. This will provide a benefit when the average packet size carried across the channel is less than 1812 bytes. For example, your CLAW performance will be improved if you are using the Cisco router to access Ethernet (standard 1500-byte frames).

If you are unsure of the average packet size carried on your CLAW links, you can estimate it for a given link by calculating the #octets/#packets ratio in both the inbound and outbound directions. These counters are accessible by using SNMP (ifInOctets, ifOutOctets, ifInUcastPkts, and ifOutUcastPkts). Refer to *z/OS Communications Server: IP System Administrator's Commands* for information about monitoring MIB objects by using SNMP.

For information about the prerequisite Cisco microcode levels, contact the Cisco support group.

Restrictions

CLAW packing is intended solely for configurations in which the CLAW link carries relatively small (less than 1812 byte) packets.

If CLAW packing is enabled, z/OS CS will enforce a maximum MTU of 1812 bytes across the channel. Therefore, you should not enable CLAW packing unless it is known that all (or the vast majority) of the packets carried across the channel are

smaller than 1812-bytes. (Throughput degradation is possible if, for example, CLAW packing is enabled on a link whose current average packet size is 4096 bytes.)

Dependencies

A CLAW router that supports the packing function is required in order for the connection to operate in packed mode. At the time of this writing, only Cisco 7200-series and 7500-series routers support CLAW packing. Check with Cisco's service group for recommended microcode levels.

What this change affects

- Performance
- Customization

Migration procedures

You do not need to change anything to operate in non-packed mode. (Non-packed mode is the default. Prior versions of CS for OS/390 enforced non-packed mode by requiring the NONE keyword on the CLAW DEVICE statement.)

If your z/OS CS is communicating with Cisco 7200- series or 7500-series routers and you determine you want to take advantage of the CLAW packing enhancement and operate in packed-mode, perform the task in the table below:

Table 101. CLAW packing within a 4K frame - Migration task

Task	Procedure	Reference
Enable packing on both the z/OS CS side and within the router.	<p>On the z/OS CS side, specify the PACKED keyword on the CLAW DEVICE statement.</p> <p>On the Cisco side, enable packing on the CLAW statement for the CIP interface. Also, reduce the IP MTU for the CIP interface to 4092 by using the IP MTU command.</p>	<p>Refer to <i>z/OS Communications Server: IP Configuration Reference</i> for information on the CLAW DEVICE statement configuration information.</p> <p>Check with Cisco for information on configuring the CLAW statement and the IP MTU command.</p>

Chapter 9. Migrating the FTP server and client

File Transfer Protocol (FTP) lets you transfer data sets between the local host and any other host that supports TCP/IP. Using the FTP command and its subcommands, you can sequentially access multiple hosts without leaving the FTP environment.

This chapter contains new and changed FTP interfaces, including:

- “FTP server configuration statements”
- “FTP client configuration statements” on page 170
- “FTP z/OS UNIX and TSO commands” on page 171
- “FTP command start options” on page 174

This chapter also contains the following for FTP:

- “z/OS V1R4 Communications Server release summary” on page 175
- “z/OS V1R2 Communications Server release summary” on page 181
- “Communications Server for OS/390 V2R10 release summary” on page 191

In general, refer to the *z/OS Communications Server: IP Configuration Guide* for details about the FTP server. For details about the FTP client, refer to the *z/OS Communications Server: IP User’s Guide and Commands*.

New and changed interfaces for FTP

FTP server configuration statements

Table 102 lists the FTP server configuration statements that are new or changed in CS for OS/390 V2R10, z/OS CS V1R2, and z/OS CS V1R4 in the *hlq.FTP.DATA* data set. For more information on these statements, refer to the *z/OS Communications Server: IP Configuration Reference*.

Table 102. New and changed FTP server configuration statements

Statement	Description	Status
ANONYMOUSLEVEL ANONYMOUSHFSFILEMODE ANONYMOUSHFSDIRMODE ANONYMOUSFILEACCESS ANONYMOUSFILETYPESEQ ANONYMOUSFILETYPESQL ANONYMOUSFILETYPEJES EMAILADDRCHECK	Statements used in anonymous FTP processing.	New in CS for OS/390 V2R10
ENCODING MBDATACONN	Statements used to support the Chinese standard GB18030 provided by codepage IBM-5488.	New in z/OS CS V1R4
FTPLOGGING ANONYMOUSFTPLOGGING	Statements used to request activity logging for non-anonymous and anonymous users.	New in z/OS CS V1R4

Table 102. New and changed FTP server configuration statements (continued)

Statement	Description	Status
BANNER LOGINMSG ANONYMOUSLOGINMSG MVSINFO ANONYMOUSMVSINFO HFSINFO ANONYMOUSHFSINFO ADMINEMAILADDRESS	Statements to support welcome pages.	New in CS for OS/390 V2R10
JESINTERFACELEVEL JESENTRYLIMIT	Statements used in filetype JES processing.	New in CS for OS/390 V2R10
CIPHERSUITE	Specifies the name of a CipherSuite that is used during the TLS handshake.	New in z/OS CS V1R2
DEBUG	Activates a specific trace type. Only one trace type can be activated for a DEBUG statement.	New in z/OS CS V1R2
	IPADDR(filter) parameter can be coded as IPv6 addresses and network prefixes as defined in RFC 2373.	Changed in z/OS CS V1R4
DEBUGONSITE	Specifies whether a client is allowed to change the server's general tracing options with a SITE DEBUG command.	New in z/OS CS V1R2
DUMP	Activates an extended trace dump ID. Only one dump ID can be activated for a DUMP statement.	New in z/OS CS V1R2
	IPADDR(filter) parameter can be coded as IPv6 addresses and network prefixes as defined in RFC 2373.	Changed in z/OS CS V1R4
DUMPSITE	Specifies whether a client is allowed to change the server's extended tracing options with a SITE DUMP command.	New in z/OS CS V1R2
EXTENSIONS	Statements to enable the FTP server to recognize FTP commands that are not described in RFC 959. EXTENSIONS AUTH_TLS allows the FTP server to select the level of TLS security. EXTENSIONS AUTH_GSSAPI specifies that the Kerberos authentication type is supported using the GSSAPI. EXTENSIONS SIZE gets byte transfer size of a file. EXTENSIONS MDTM gets the time a file was last modified. EXTENSIONS REST_STREAM enables the FTP server to restart stream mode file transfers. EXTENSIONS UTF8 enables the FTP server to respond to the LANG command, and to use UTF8 encoding of pathnames on the control connection.	New in CS for OS/390 V2R10; changed in z/OS CS V1R2
ISPFSTATS	Statement that creates and maintains statistics for partitioned data set members. It can be set to TRUE or FALSE.	New in z/OS CS V1R2
KEYRING	Required if TLS is used for encryption or authentication. It defines the keyring that contains the certificate to be used during the TLS handshake.	New in z/OS CS V1R2

Table 102. New and changed FTP server configuration statements (continued)

Statement	Description	Status
MVSURLKEY	Statement to define the key used to indicate an MVS data set name in a Web site.	New in CS for OS/390 V2R10
PORTCOMMAND PORTCOMMANDPORT PORTCOMMANDIPADDR	<p>The PORTCOMMAND statement specifies whether PORT command will be rejected or accepted. This will prevent an FTP client in session with this server from successfully executing any subcommand that requires the PORT command.</p> <p>The PORTCOMMANDPORT statement specifies what range of port values the server will accept as a parameter for the PORT command.</p> <p>The PORTCOMMANDIPADDR directs the server to accept only PORT commands that have an IP address that matches that of the client.</p>	New in z/OS CS V1R2
	The existing statements PORTCOMMAND, PORTCOMMANDPORT, and PORTCOMMANDIPADDR now apply to the EPRT command as well as the PORT command.	Changed in z/OS CS V1R4
SBSUB SBSUBCHAR	Statements used when specifying substitution characters for non-translatable characters.	New in z/OS CS V1R4
SECURE_*	<p>Statements to allow the FTP server to select the level of security.</p> <p>SECURE_FTP specifies whether authentication is required. This keyword is only valid if EXTENSIONS AUTH_TLS is specified.</p> <p>SECURE_LOGIN sets the authorization level required for users.</p> <p>SECURE_CTRLCONN specifies the minimum level of security allowed for the control connection.</p> <p>SECURE_DATACONN specifies the minimum level of security required on the data connection.</p> <p>SECURE_PBSZ specifies the maximum size of the encoded data blocks sent during file transfer.</p>	New in z/OS CS V1R2
TLSTIMEOUT	Provides a unique timeout value for TLS handshake processing. This timeout is the maximum number of seconds between the long form of TLS handshakes.	New in z/OS CS V1R2
SMF SMFAPPE SMFDEL SMFEXIT SMFJES SMFLOGN SMFREN SMFRETR SMFSQL SMFSTOR	Specifies SMF recording options.	Changed in z/OS CS V1R2

Table 102. New and changed FTP server configuration statements (continued)

Statement	Description	Status
VCOUNT UCOUNT VOLUME	Statements to allow data to span multiple volumes.	VCOUNT and UCOUNT are new in CS for OS/390 V2R10. VOLUME is changed in CS for OS/390 V2R10.

FTP client configuration statements

Table 103 lists the FTP client configuration statements that are new or changed in CS for OS/390 V2R10, z/OS CS V1R2, and z/OS CS V1R4 in the *hlq.FTP.DATA* data set. For more information on these statements, refer to the *z/OS Communications Server: IP Configuration Reference*.

Table 103. New and changed FTP client configuration statements

Statement	Description	Status
CIPHERSUITE	Specifies the name of a CipherSuite that is used during the TLS handshake.	New in z/OS CS V1R2
DEBUG	Activates a specific trace type. Only one trace type can be activated for a DEBUG statement.	New in z/OS CS V1R2
DUMP	Activates an extended trace dump ID. Only one dump ID can be activated for a DUMP statement.	New in z/OS CS V1R2
ENCODING MBDATACONN	Statements used to support the Chinese standard GB18030 provided by codepage IBM-5488.	New in z/OS CS V1R4
ISPFSTATS	Statement that creates and maintains statistics for partitioned data set members. It can be set to TRUE or FALSE.	New in z/OS CS V1R2
KEYRING	Required if TLS is used for encryption or authentication. It defines the keyring that contains the certificate to be used during the TLS handshake.	New in z/OS CS V1R2
PRIVATE	Sets the security protection level for data transfers to private.	New in z/OS CS V1R2
PROTECT parm	Sets the security protection level for data transfers to the value (clear, safe, or private) specified as a parameter.	New in z/OS CS V1R2
SAFE	Sets the security protection level for data transfers to safe.	New in z/OS CS V1R2
SBSUB SBSUBCHAR	Statements used when specifying substitution characters for non-translatable characters.	New in z/OS CS V1R4

Table 103. New and changed FTP client configuration statements (continued)

Statement	Description	Status
SECURE_* statements	<p>Statements to allow the FTP client to select the level of security.</p> <p>SECURE_MECHANISM TLS specifies that TLS is the security mechanism that is used by the client when it sends an AUTH command. SECURE_MECHANISM GSSAPI specifies that the Kerberos authentication type is supported using the GSSAPI.</p> <p>SECURE_FTP specifies that authentication is required. This means that the FTP client must send an AUTH command before the client can log in.</p> <p>SECURE_CTRLCONN specifies the minimum level of security allowed for the control connection.</p> <p>SECURE_DATACONN specifies the minimum level of security required on the data connection.</p> <p>SECURE_PBSZ specifies the maximum size of the encoded data blocks sent during file transfer.</p>	New in z/OS CS V1R2
SOCKSCONFIGFILE	Configuration file or data set that enables the FTP client to connect to an FTP server by means of a SOCKS server.	New in z/OS CS V1R2
TLSTIMEOUT	Provides a unique timeout value for TLS handshake processing. This timeout is the maximum number of seconds between the long form of TLS handshakes.	New in z/OS CS V1R2
VCOUNT UCOUNT VOLUME	Statements to allow data to span multiple volumes.	VCOUNT and UCOUNT are new in CS for OS/390 V2R10. VOLUME is changed in CS for OS/390 V2R10.

FTP z/OS UNIX and TSO commands

Table 104 lists the changes made to the FTP z/OS UNIX and TSO commands in CS for OS/390 V2R10, z/OS CS V1R2, and z/OS CS V1R4. For more information on z/OS UNIX and TSO commands, including FTP subcommands, refer to the *z/OS Communications Server: IP User's Guide and Commands* and *z/OS Communications Server: IP System Administrator's Commands*.

Table 104. FTP z/OS UNIX and TSO commands

Command or parameter	Description	Status
CCC	Sets the security protection level for commands to clear.	New in z/OS CS V1R2
CLEAR	Sets the security protection level for data transfers to clear.	New in z/OS CS V1R2
CPROTECT parm	Sets the security protection level for commands to the value (clear, safe, or private) specified as a parameter.	New in z/OS CS V1R2
DEBUG	Activates one or more general trace types.	Changed in z/OS CS for V1R2
DIR	Command to display directory contents. Changed to suppress display of data sets to which the user has no access.	Changed in z/OS CS for V1R2
DUMP	Activates one or more extended trace dump IDs.	New in z/OS CS for V1R2
FEAT	Command that queries the FTP server to find out which features it supports.	New in z/OS CS for V1R2

Table 104. FTP z/OS UNIX and TSO commands (continued)

Command or parameter	Description	Status
foreign-host	FTP client start option. In z/OS CS V1R4, it can be specified as an IPv6 address.	Changed in z/OS CS V1R4
host-name	FTP client subcommand open parameter. In z/OS CS V1R4, host-name can be specified as an IPv6 address.	Changed in z/OS CS V1R4
LANG	Command that sets the language used for FTP replies from the server.	New in z/OS CS for V1R2
LOCSITE	Options to allow data to span multiple volumes: VCOUNT, UCOUNT, and VOLUME.	VCOUNT and UCOUNT were new in CS for OS/390 V2R10; VOLUME was changed in CS for OS/390 V2R10
	ISPFSTATS and NOISPFSTATS parameters added to allow (or disallow) FTP to create or update ISPF member statistics when GET or MGET subcommands are issued.	New in z/OS CS V1R2
	New subcommand parameters to support the Chinese standard GB18030 provided by codepage IBM-5488: ENCODING and MBDATACONN. Also new SBSUB and SBSUBCHAR parameters for substitution for single-byte translations.	New in z/OS CS for V1R4
LOCSTAT	Additional options supported: <ul style="list-style-type: none"> • AUTOTAPEMOUNT • CCONNTIME • DATACTTIME • DCONNTIME • INACTTIME • MYOPENTIME • VCOUNT • UCOUNT • VOLUME 	Changed in CS for OS/390 V2R10
	Additional options supported: <ul style="list-style-type: none"> • ENCODING • MBDATACONN • SBSUB • SBSUBCHAR 	New in z/OS CS for V1R4
MGET, MPUT, and MDEL	Commands to get, put, or delete multiple files. Changed to suppress display of data sets that the user cannot access.	Changed in z/OS CS for V1R2

Table 104. FTP z/OS UNIX and TSO commands (continued)

Command or parameter	Description	Status
MODIFY	<p>The MODIFY command has two new parameters: DEBUG= for general tracing and DUMP= for extended tracing. Values are required on the MODIFY DUMP and the MODIFY DEBUG command. The following are the equivalent specifications of the old parameters that were available on the MODIFY command (the old specifications are to the left of the arrow, the new are on the right of the arrow):</p> <ul style="list-style-type: none"> • modify jobname,TRACE ==>modify jobname,DEBUG=(BAS) • modify jobname,NOTRACE ==>modify jobname,DEBUG=(NONE) • modify jobname,JTRACE ==>modify jobname,DEBUG=(CMD,FSC,JES) • modify jobname,NOJTRACE ==>modify jobname,DEBUG=(NONE) • modify jobname,NODUMP ==>modify jobname,DUMP=(NONE) • modify jobname,JDUMP ==>modify jobname,DUMP=(JES) • modify jobname,NOJDUMP ==>modify jobname,DUMP=(NONE) <p>In addition, the following are no longer supported:</p> <ul style="list-style-type: none"> • modify jobname,UTRACE • modify jobname,NOUTRACE 	New in z/OS CS for V1R2
	MODIFY ftpjobname,DEBUG=IPADDR(filter) now accepts IPv6 addresses and network prefixes as defined in RFC 2373.	Changed in z/OS CS for V1R4
OPTS	Command to set command options.	New in z/OS CS for V1R2
PRIVATE	Sets the security protection level for data transfers to private.	New in z/OS CS V1R2
PROTECT parm	Sets the security protection level for data transfers to the value (clear, safe, or private) specified as a parameter.	New in z/OS CS V1R2
SAFE	Sets the security protection level for data transfers to safe.	New in z/OS CS V1R2

Table 104. FTP z/OS UNIX and TSO commands (continued)

Command or parameter	Description	Status
SITE	New options for filetype JES processing: <ul style="list-style-type: none"> • JESOWNER • JESENTRYLIMIT • JESSTATUS • JESJOBNAME New options to allow data to span multiple volumes: <ul style="list-style-type: none"> • VCOUNT • UCOUNT Changed option: <ul style="list-style-type: none"> • VOLUME 	Changed in CS for OS/390 V2R10
	DUMP option controls the server's extended trace.	New in z/OS CS for V1R2
	DEBUG option controls the server's trace.	New in z/OS CS for V1R2
	ISPFSTATS and NOISPFSTATS parameters added to allow (or disallow) FTP to create or update ISPF member statistics when GET or MGET subcommands are issued.	New in z/OS CS for V1R2
	New subcommand parameters to support the Chinese standard GB18030 provided by codepage IBM-5488: ENCODING and MBDATACONN. Also new SBSUB and SBSUBCHAR parameters for substitution for single-byte translations.	New in z/OS CS for V1R4
SRESTART	Command to restart an interrupted stream mode file transfer.	New in z/OS CS for V1R2
STAT	Additional options supported: <ul style="list-style-type: none"> • ENCODING • MBDATACONN • SBSUB • SBSUBCHAR 	New in z/OS CS for V1R4
VERBOSE	Toggles the display of message IDs when the FTP client is running in the z/OS UNIX environment.	New in z/OS CS for V1R2

FTP command start options

Table 105 lists the changes made to the FTP command start options in CS for OS/390 V2R10, z/OS CS V1R2, and z/OS CS V1R4. For more information on the server FTP command start options, refer to *z/OS Communications Server: IP User's Guide and Commands*. For more information on the client FTP command start options, refer to *z/OS Communications Server: IP Configuration Reference*.

Table 105. FTP command start options

Parameter	Description	Status
-a GSSAPI	For Kerberos support; used when FTP attempts to authenticate to the FTP server by sending the AUTH command specifying GSSAPI as the authentication type.	New in z/OS CS V1R2
-A GSSAPI	The -A options were changed to -r options. See the -r GSSAPI entry in this table.	New in z/OS CS V1R2; made obsolete in z/OS CS V1R4
-a TLS	For TLS enablement; used when the FTP client attempts authentication upon initial connection by sending the AUTH TLS command.	New in z/OS CS V1R2
-A TLS	The -A options were changed to -r options. See the -r TLS entry in this table.	New in z/OS CS V1R2; made obsolete in z/OS CS V1R4

Table 105. FTP command start options (continued)

Parameter	Description	Status
-a NEVER	For Kerberos support and TLS enablement; FTP will not attempt auto-authentication upon initial connection.	New in z/OS CS V1R2
-A NEVER	The -A options were changed to -r options. See the -r NEVER entry in this table.	New in z/OS CS V1R2; made obsolete in z/OS CS V1R4
-r GSSAPI	In z/OS CS V1R2, this was the -A GSSAPI option. This option is for Kerberos support; used when FTP attempts to authenticate to the FTP server by sending the AUTH command specifying GSSAPI as the authentication type. The option -r is the same as -a except that the AUTH command must be accepted by the server. If it is not, then the client ends the session.	New in z/OS CS V1R4
-r NEVER	In z/OS CS V1R2, this was the -A NEVER option. This option is for Kerberos support and TLS enablement; FTP will not attempt auto-authentication upon initial connection.	New in z/OS CS V1R4
-r TLS	In z/OS CS V1R2, this was the -A TLS option. This option is for TLS enablement; used when the FTP client attempts authentication upon initial connection by sending the AUTH TLS command. The option -r is the same as -a except that the AUTH command must be accepted by the server. If it is not, then the client ends the session.	New in z/OS CS V1R4
-x	For Kerberos support; causes the client to attempt to negotiate encryption (data and command protection levels "private") immediately after successfully authenticating.	New in z/OS CS V1R2
foreign-host	An FTP client start option. In z/OS CS V1R4, can specified as an IPv6 address.	Changed in z/OS CS V1R4

z/OS V1R4 Communications Server release summary

This section describes the FTP functions new in z/OS V1R4 Communications Server.

FTP support for substitution characters during EBCDIC/ASCII single-byte translations

Prior to this release, if a character in the input stream did not map to the file system code set during a file transfer, FTP would fail the transfer. z/OS V1R4 Communications Server allows you to configure FTP to use substitution characters for non-translatable characters, thus avoiding failed transfers.

Restrictions

If a substitution occurs during a file transfer, you cannot restore the original file by reversing the order of file transfer.

What this change affects

- Operations

Migration procedures

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 106. FTP support for substitution characters during EBCDIC/ASCII single-byte translations - Migration tasks

Task	Procedure	Reference
Enable FTP to substitute characters that cannot be translated.	In FTP.DATA, specify SBSUB TRUE.	<i>z/OS Communications Server: IP Configuration Reference</i>
Specify the single-byte substitution character in a hexadecimal format that will be used for substitution.	In FTP.DATA, specify a single-byte character, in a hexadecimal format, to a SBSUBCHAR keyword.	<i>z/OS Communications Server: IP Configuration Reference</i>
After logging in to FTP, enable FTP to substitute for characters that cannot be translated (for the current session only).	Perform the following steps: <ul style="list-style-type: none"> • Issue SITE and LOCSITE subcommands with the SBSUBCHAR parameter to specify the substitution character. • Issue SITE and LOCSITE subcommands with the SBSUB=TRUE parameter. 	<i>z/OS Communications Server: IP User's Guide and Commands</i>

Enhanced FTP activity logging

In z/OS V1R4 Communications Server, the FTP server is enhanced with improved diagnostic information recorded in the SYSLOGD file. The information uses message numbers that are documented in *z/OS Communications Server: IP Messages Volume 3 (EZY)* and allows for correlation of information recorded for an FTP session. The enhanced FTP activity logging provides the system programmer with standardized information for resolving FTP problems and for tracking usage of the services of the FTP server.

Restrictions

None.

Dependencies

SYSLOGD must be started.

What this change affects

- Diagnosis

Migration procedures

This function does not require any action unless you want to take advantage of the function. If so, perform the appropriate task in the following table.

Table 107. Enhanced FTP activity logging - Migration tasks

Task	Procedure	Reference
Request activity logging for non-anonymous users.	In the FTP.DATA file for the server, code: FTPLOGGING TRUE.	<i>z/OS Communications Server: IP Configuration Reference</i>
Request activity logging for anonymous users.	In the FTP.DATA file for the server, code: ANONYMOUSFTPLOGGING TRUE.	<i>z/OS Communications Server: IP Configuration Reference</i>

Changed behavior of login failure replies

z/OS V1R4 Communications Server changes the default behavior of password failure replies. When the PASS command fails, the FTP server will now reply to the client with minimal information about why the PASS command failed. This is an enhancement to the previous behavior because this change prevents sensitive information about USERIDs and PASSWORDS from being exposed to the end user.

Note: This update is available in z/OS V1R2 CS with APAR PQ51780.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

This update does not require any action. The change is automatic (the default for the FTP.DATA keyword ACCESSERRORMSGs is FALSE). If you want to override the default and reply to the client with detailed PASS command failure information, perform the first task in the following table. If you want to prevent password failure information from being returned to the client, yet record error information for diagnostic purposes, then perform the second task in the table.

Table 108. Changed behavior of login failure replies - Migration tasks if you want to override default behavior

Task	Procedure	Reference
Override the new default behavior and obtain detailed information for password failure replies.	Do one of the following: <ul style="list-style-type: none">• Configure the FTP server to send additional information by setting the FTP.DATA keyword ACCESSERRORMSGs to TRUE. This will send detailed login failure information that includes the function call that failed and its return and reason code.• Turn on the DEBUG option called ACC to log the error messages in the syslog.	<i>z/OS Communications Server: IP Configuration Reference</i>
Prevent password failure information from being returned to the client, yet record error information for diagnostic purposes.	Turn on the DEBUG option ACC to log the error information in the syslog.	<i>z/OS Communications Server: IP Diagnosis and z/OS Communications Server: IP Configuration Reference</i>

Support for Chinese standard GB18030 provided by codepage IBM-5488

z/OS V1R4 Communications Server allows FTP to transfer files that are encoded in the IBM-5488 codepage.

Restrictions

The support requires that the following FTP protocols are in use at the time of a data transfer:

Protocol	Type
Structure	FILE
Transmission mode	STREAM
Data type	ASCII

In addition, the following additional restrictions are enforced when the support is used:

- The FILETYPE setting must be SEQ.
- If the file transferred is an MVS data set, its record format (RECFM) must be V, VB, or U.
- If the file transferred is an MVS data set with RECFM=V or RECFM=VB and the transfer is outbound, then requesting RDWs is not allowed.

- For the FTP server, the SIZE command is not allowed.
- For the FTP client, the transfer must not be part of the SRESTART subcommand.

What this change affects

- Customization

Migration procedures

The support for Chinese standard GB18030 provided by codepage IBM-5488 function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 109. Support for Chinese standard GB18030 provided by codepage IBM-5488 - Migration tasks

Task	Procedure	Reference
Choose the IBM-5488 codepage for the FTP server's data connection translate table.	In the server's FTP.DATA file, code ENCODING MBCS and code MBDATACONN (IBM-1388,IBM-5488).	<i>z/OS Communications Server: IP Configuration Reference</i>
Choose the IBM-5488 codepage for the FTP client's data connection translate table.	In the client's FTP.DATA file, code ENCODING MBCS and code MBDATACONN (IBM-1388,IBM-5488).	<i>z/OS Communications Server: IP User's Guide and Commands</i>
Change data connection translation tables to the IBM-5488codepage during an FTP client/server session.	Change server's translation table by issuing SITE ENCODING=MBCS and by issuing SITE MBDATACONN=(IBM-1388,IBM-5488). Change client's translation table by issuing LOCSITE ENCODING=MBCS and by issuing LOCSITE MBDATACONN=(IBM-1388,IBM-5488).	<i>z/OS Communications Server: IP User's Guide and Commands</i>

Enhancements to FTP server user exits

z/OS V1R4 Communications Server allows FTP exits to support IPv6 local and remote addresses and also allows implementation of more comprehensive FTP server security exit functions. The following enhancements to FTP user exits are introduced:

- New samples are provided for all exits.
The new samples of all the changed exits are provided in SEZAINST. The samples FTCHKCM1 and FTCHKCM2 are also updated. The SEZAINST(FTPOSTPR) exit was added in CS for OS/390 V2R10 in the C language. In z/OS V1R4 CS, a new sample called SEZAINST(FTPOSTPA) is included in the Assembler language.
- Bytes transferred and data set name are now passed to FTPOSTPR.
- Client and server IP addresses now include support for IPv6 addresses in all exits except FTPSMFEX user exit. The FTPSMFEX user exit is unchanged because it utilizes the old SMF Type 118 record instead of the preferred SMF Type 119 record.
- A scratchpad area is available for communicating between exits.
The 256-byte scratchpad area can be used to communicate between the exits that have access to it. It is not altered by FTP after its initial allocation and it persists as long as the session for this user remains active. The contents are lost if the session switches to a new userid or logs off. It may contain any data within the 256 bytes. Some potential uses for the scratchpad are counting the number

of attempts by a user to access a resource, passing information from one exit to another to control processing, or even using STCK to time the execution of a command.

The following table provides a list of the parameters and the exits that are affected.

Table 110. FTP parameters and user exits that are enhanced in z/OS CS V1R4

Parameter	User Exit
Buffer to hold 500- reply extension	FTCHKCMD
Number of bad passwords in this login attempt	FTCHKPWD
Name of data set or HFS file stored or retrieved	FTPOSTPR
Total bytes transferred	FTPOSTPR
Scratchpad buffer to communicate with other exits	FTCHKCMD, FTCHKJES, FTPOSTPR
Client's socket address structure	All but FTPSMFEX
Server's socket address structure	All but FTPSMFEX
Session instance identifier used in logging messages for this session	All but FTPSMFEX

Restrictions

The following restrictions apply:

- The z/OS V1R4 CS enhanced FTP user exit interface is compatible with user exits from prior releases. The old user exits can run as is, or they can be modified to take advantage of the z/OS V1R4 CS parameters. FTCHKIP and FTPOSTPR may continue to reference their existing IP address fields for IPv4 addresses and IPv4 addresses mapped into IPv6 format. Once the exits are used with true IPv6 addresses, the new socket address structure parameters must be used instead.
- The two user exits that are loaded prior to the spawning of the final process (FTCHKIP and FTCHKPWD) will not have access to the scratchpad.

What this change affects

- Customization
- Installation
- Security
- Usability

Migration procedures

The enhancements to FTP server user exits do not require any action unless you want to take advantage of the new information passed to the exits. If so, perform the tasks in the following table.

Table 111. Enhancements to FTP server user exits - Migration tasks

Task	Procedure	Reference
Modify existing exits to use the new interface (required only to use the new parameters).	Use the provided samples for each exit to update the calling parameter list for each exit and to access the new parameters in the list.	<i>z/OS Communications Server: IP Configuration Reference</i> and SEZAINST sample library

Table 111. Enhancements to FTP server user exits - Migration tasks (continued)

Task	Procedure	Reference
Modify exits to utilize the new parameters.	Use the provided samples or your modified exits as a base. To these exits, add instructions that make decisions based on the new parameters, such as rejection of login based on IP address, tracking number of bytes for all transfers, and customizing a 500- reply to explain why a command was rejected by FTCHKCMD.	<i>z/OS Communications Server: IP Configuration Reference</i> , <i>z/OS MVS Programming: Authorized Assembler Services Guide</i> , and SEZAINST sample library
Ensure proper authorization.	The user exit load modules must be placed in an APF-authorized library to which the FTP server has access by way of STEPLIB, linklist, or LPA. Also, the authorization state (JSCBAUTH) must be the same after exiting from the user exit as it was upon entry. If a user exit is not found, processing proceeds as though a return code of 0 was received from the user exit call.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS MVS Initialization and Tuning Reference</i>

IPv6 support for FTP

Prior to this release, a z/OS FTP client could not communicate with an FTP server on an IPv6 node, nor could the z/OS FTP server accept connections from clients executing on IPv6 nodes. In z/OS CS V1R4, IPv6 support is added to FTP to make IPv6 connectivity possible for both the FTP client and server.

RFC 2428 implementation is part of the IPv6 enhancement.

Restrictions

The following restrictions apply:

- The FTP client SOCKSCONFIGFILE is never referenced by the client when connecting to an FTP server with an IPv6 IP address.
- In the SOCKSCONFIGFILE, you cannot specify the DNS name of a SOCKS server on an IPv6 node unless the IPv6 node is multihomed and accessible from an IPv4 network.
- Proxy transfer between mixed protocol FTP servers (that is, between a server known to the FTP client as an IPv6 node and a server known to the FTP client as an IPv4 node), will succeed only if the primary server can connect to the secondary server using the same protocol as the secondary server's control connection.
- The FTP server does not allow the EPSV command to specify a protocol for the data connection different from the protocol used for the control connection.
- The FTP server does not allow the EPRT command to specify a protocol for the data connection different from the protocol used for the control connection.
- The FTP server does not accept the PORT command when the control connection is IPv6.
- Kerberos protection of IPv6 connections is not supported by either client or server.
- For IPv6 connection partners, RACF does not validate the login. RACF does not prevent any IPv6 connection partner from accessing the server.

Incompatibilities

z/OS FTP will not be able to use IPv6 connections unless at least one TCP/IP stack on your system supports IPv6 networking. The z/OS TCP/IP stack does not support IPv6 networking unless you define it to UNIX System Services as an AF_INET6 network.

Dependencies

To use this function, you must have an IPv6 enabled TCP/IP, such as z/OS V1R4 TCP/IP configured as an AF_INET6 network.

What this change affects

- Operations
- Availability
- Diagnosis
- Usability

Migration procedures

This function does not require any action unless you want your FTP server or client to operate with IPv6 networks. If so, perform the tasks in the following table.

Table 112. IPv6 application for FTP - Migration tasks

Task	Procedure	Reference
Enable FTP server to accept connections from IPv6 nodes as well as IPv4 nodes.	Configure z/OS TCP/IP (or any other TCP/IP stack) as an AF_INET6 network.	<i>z/OS Communications Server: IPv6 Network and Application Design Guide</i>
Enable FTP client to connect to FTP server on an IPv6 node.	Do the following: <ol style="list-style-type: none">1. Configure client host z/OS TCP/IP (or any other TCP/IP stack) as an AF_INET6 network.2. Update hostname files to define host names for IPv6 server hosts (This is optional. You can always specify the FTP server as an IP address instead of a host name).	<i>z/OS Communications Server: IPv6 Network and Application Design Guide, z/OS Communications Server: IP Configuration Reference, and z/OS Communications Server: IP Configuration Guide</i>
Connect to FTP server on an IPv6 node.	Use FTP client foreign-host start option, or use the OPEN subcommand hostname parameter, to specify the IPv6 FTP server.	<i>z/OS Communications Server: IP User's Guide and Commands</i>

z/OS V1R2 Communications Server release summary

This section describes the FTP functions new in z/OS V1R2 Communications Server.

Security enhancements

Enhancing FTP server security

z/OS V1R2 Communications Server provides new FTP.DATA statements to enhance server security by protecting against bounce attacks. The *bounce attack* occurs when an FTP PORT command is sent to an FTP server that contains the network address and the port number of the machine and service being attacked. Instructing a third party to connect to the service and to send a file, rather than connecting directly, makes tracking down the perpetrator difficult and can circumvent network address-based access restrictions.

Furthermore, an FTP client can establish a data connection to any server, even a server that is not FTP, that is listening to a port. If the client sent a large amount of unexpected data to a non-FTP server, the server could experience disruption. The new FTP.DATA statements prevent your server from being used in this way by allowing you to reject a port command.

There are new messages and codes for this function. Refer to *z/OS Communications Server: IP Messages Volume 3 (EZY)* for information on the messages and refer to *z/OS Communications Server: IP and SNA Codes* for information on codes.

Refer to *z/OS Communications Server: IP Configuration Guide* for more discussion about using FTP server security in PROXY mode.

Dependencies: In order for PORTCOMMANDIPADDR or PORTCOMMANDPORT keywords to have any effect, PORTCOMMAND must be specified to ACCEPT. (PORTCOMMAND ACCEPT is the default.)

Migration procedures: The enhancing FTP server security function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 113. Enhancing FTP server security - Migration tasks

Task	Procedure	Reference
Reject all PORT commands.	Specify the PORTCOMMAND parameter as REJECT in the server FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Reject PORT commands with port numbers less than 1024.	Specify PORTCOMMANDPORT as NOLOWPORTS in the server FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Reject PORT commands if the IP address on the PORT does not match the client IP address of the control connection.	Specify PORTCOMMANDIPADDR as NOREDIRECT in server FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Reject all PORT commands that specify an IP address other than the client's own IP address or port numbers that are well-known.	Specify the following in the server FTP.DATA: <ul style="list-style-type: none"> • PORTCOMMANDIPADDR • NOREDIRECT • PORTCOMMANDPORT • NOLOWPORTS 	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Restrict DIR output

z/OS V1R2 Communications Server enhances system integrity to allow the FTP server to honor catalog security as defined by an installation. The FTP server provides catalog security where users cannot list the names of data sets that are contained in catalogs to which they do not have read access. This is consistent with the way ISPF data set list works (ISPF option 3.4). If your installation has catalog read protection defined, and relies on the fact that users can list data set names in such protected catalogs, you will see changed behavior for FTP commands using catalog listing information, such as the DIR, MGET, MPUT, and MDEL commands.

Only data sets that are cataloged in catalogs to which you have read access will be included in output from these commands. Your installation may want to define additional security profiles that allow read access to certain catalogs. There are no changes to the use of security profiles for accessing the actual data sets.

Migration procedures: There are no migration procedures for the restrict DIR output function; it is automatically enabled.

Surrogate RACF support

In CS for OS/390 V2R10, a new keyword, anonymouslevel 3, was introduced; see “Server anonymous enhancements” on page 194. z/OS V1R2 Communications Server enhances security in the FTP server when using ANONYMOUSELEVEL 3 by allowing you to specify a surrogate password instead of being required to enter a password in plain text. This is accomplished with a new ANONYMOUS option in the FTP.DATA server configuration file.

Migration procedures: The surrogate RACF support function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 114. Surrogate RACF support - Migration tasks

Task	Procedure	Reference
Enable the FTP server to process users without passwords.	<p>Perform the following steps from TSO.</p> <ol style="list-style-type: none"> 1. Activate the SURROGAT class support in RACF by entering the following RACF commands: SETROPTS CLASSACT(SURROGAT) SETROPTS RACLIST(SURROGAT) 2. Issue a REFRESH command after any changes to the SURROGAT profiles if the SURROGAT profile is in the RACLIST. For example, to create the SURROGAT class profile for user GUEST, issue: RDEFINE SURROGAT BPX.SRV.GUEST UACC(NONE) SETROPTS RACLIST(SURROGAT) REFRESH <p>Note that a similar SURROGAT profile is required for each user ID that a server must support without a password.</p> <ol style="list-style-type: none"> 3. Issue a PERMIT command to allow the user ID of the FTP daemon (such as FTPD) to create a security environment for the user GUEST: PERMIT BPX.SRV.GUEST CLASS(SURROGAT) ID(FTPD) ACCESS(READ) SETROPTS RACLIST(SURROGAT) REFRESH 	<p><i>z/OS Communications Server: IP Configuration Guide and z/OS Security Server RACF Security Administrator's Guide</i></p>
Enable the SURROGAT function for an anonymous user of the FTP server.	<p>In the server FTP.DATA, include the following statement: ANONYMOUS userid/SURROGATE ANONYMOUSLEVEL 3</p>	<p><i>z/OS Communications Server: IP Configuration Reference</i></p>

Socksify FTP client

z/OS V1R2 Communications Server allows you to use the z/OS CS FTP client to connect to FTP servers that reside beyond a firewall that runs a SOCKS server. The SOCKS server may be either a SOCKS Version 4 or a SOCKS Version 5 server.

Restrictions: The following restrictions apply:

- Only the z/OS CS FTP client is socksified.
- The z/OS CS FTP client only uses one of the SOCKS V5 authentication methods described in RFC 1928:

NO_AUTHENTICATION_REQUIRED.

- The IDENTD authentication is not supported.
- Any server tracing that identifies the client IP address will show the IP address of the SOCKS server, rather than the IP address of the client.
- Any exit routines driven with the IP address of the FTP client will be driven with the IP address of the SOCKS server, rather than the IP address of the client.

Migration procedures: The socksify FTP client function does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 115. Socksify FTP client - Migration Task

Task	Procedure	Reference
Enable the FTP client to connect to an FTP server by means of a SOCKS server.	<ol style="list-style-type: none"> 1. Create the SOCKS.CNF configuration data set or file and enter the required configuration data. 2. Specify the SOCKS.CNF configuration filepath in FTP.DATA by using the keyword SOCKSCONFIG file. 	<i>z/OS Communications Server: IP Configuration Guide and z/OS Communications Server: IP Configuration Reference</i>

TLS enablement for FTP

File data transferred between an FTP client and server should be secured with respect to encryption, authentication, and data integrity. The Transport Layer Security (TLS) enablement for FTP function allows you to specify this level of security without requiring an end-to-end (client to server) IPsec infrastructure to be in place.

Restrictions: None.

Migration procedures: The TLS enablement for FTP function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 116. TLS enablement for FTP - Migration tasks

Task	Procedure	Reference
Customize the FTP server to allow or require TLS security.	Specify new EXTENSIONS AUTH_TLS and the SECURE_* statements to select the level of TLS security.	<i>z/OS Communications Server: IP Configuration Guide and z/OS Communications Server: IP Configuration Reference</i>
Customize the FTP client to allow or require TLS security.	Specify new SECURE_MECHANISM and the SECURE_* statements to select the level of TLS security.	<i>z/OS Communications Server: IP Configuration Guide and z/OS Communications Server: IP Configuration Reference</i>
Install key rings with certificates for the client and the server.	Use utility programs that are designed to create and install key rings.	<i>z/OS Communications Server: IP Configuration Guide and z/OS Communications Server: IP System Administrator's Commands</i>

Kerberos support for the FTP server and client

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications using secret-key cryptography. The Kerberos support provided in z/OS V1R2 Communications Server provides greater security for certain applications and allows the use of these applications to secure data traffic in the network. Specifically, z/OS V1R2 Communications Server introduces Kerberos support for authentication for the following applications:

- The UNIX remote shell execution (rsh) server — authentication support provided by the Kerberos 5 protocol and the GSSAPI protocol
- The FTP client and FTP server — authentication support provided by the GSSAPI protocol.
- The UNIX Telnet server— authentication support provided by the Kerberos 5 protocol

If you are using UNIX Telnet, FTP, or UNIX RSHD, you must add these Kerberos data sets:

- EUVF.SEUVFLNK - add to the LNKLSTxx PARMLIB member
- EUVF.SEUVFLPA - add to the LPALSTxx PARMLIB member

The Kerberos support for the FTP client and FTP server is described in this section. See “z/OS UNIX RSHD Kerberos support” on page 111 for the UNIX RSHD server considerations. See “z/OS UNIX Telnet (otelnets) server – Kerberos support” on page 216 for the UNIX Telnet server considerations.

Restrictions: None.

Incompatibilities: The zSeries KDC is incompatible with Windows 2000 Kerberos applications. Windows 2000 applications must use the Windows KDC. To support Windows 2000 applications, a cross-realm connection between the zSeries KDC and the Windows KDC is required.

Migration procedures: The Kerberos support for the FTP server and client function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table. See “z/OS UNIX RSHD Kerberos support” on page 111 for the UNIX RSHD server considerations. See “z/OS UNIX Telnet (otelnets) server – Kerberos support” on page 216 for the UNIX Telnet server considerations.

Table 117. Kerberos support for the FTP server and client - Migration tasks

Task	Procedure	Reference
Enable GSSAPI authentication in the FTP client.	Specify the -a parameter when invoking the FTP client or add the SECURE_MECHANISM GSSAPI keyword to the FTP.DATA file.	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Enable automatic encryption negotiation in the FTP client.	Specify the -x parameter when invoking the FTP client.	<i>z/OS Communications Server: IP User's Guide and Commands</i>
Enable GSSAPI authentication in the FTP server.	Specify the EXTENSIONS AUTH_GSSAPI keyword in the FTP.DATA file.	<i>z/OS Communications Server: IP Configuration Reference</i>
Require GSSAPI authentication in the FTP client.	Specify the -r parameter when invoking the FTP client or add the SECURE_FTP REQUIRED keyword to the FTP.DATA file.	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Table 117. Kerberos support for the FTP server and client - Migration tasks (continued)

Task	Procedure	Reference
Require GSSAPI authentication in the FTP server.	Specify the SECURE_FTP REQUIRED keyword in the FTP.DATA file.	<i>z/OS Communications Server: IP Configuration Reference</i>
Disable GSSAPI authentication in the FTP client.	Specify the -a NEVER or -A NEVER parameter when invoking the FTP client or remove the SECURE_MECHANISM GSSAPI from the FTP.DATA file.	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Disable GSSAPI authentication in the FTP server.	Remove the EXTENSIONS AUTH_GSSAPI keyword from the FTP.DATA file.	<i>z/OS Communications Server: IP Configuration Reference</i>

Functional enhancements

ISPF statistics

ISPF statistics give useful information about PDS files, such as date created, size, and date last modified. These statistics now can be created or updated by FTP when transferring files by using SITE/LOCSITE subcommands or by setting the keyword in FTP.DATA.

Restrictions and Considerations: The following restrictions or considerations apply when creating or updating ISPF statistics using FTP by using SITE/LOCSITE subcommands or by setting the keyword in FTP.DATA:

- ISPF statistics are only given for members of partitioned data sets.
- Record format must be one of the following:
 - V (Variable, Unblocked)
 - VB (Variable Blocked)
 - F (Fixed Unblocked)
 - FB (Fixed Blocked)
- Record length must be less than 256.
- PDS Member's ISPF statistic, MOD, will be set to 0 because this statistic cannot be determined by FTP.
- Behavior of file transfer of PDS member to PDS member in block mode or in compress mode will not change.
- If you want to preserve the statistics of a PDS member that already has statistics, IBM recommends that you transfer in block mode or in compress mode.

Migration procedures: The ISPF statistics function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 118. ISPF statistics - Migration tasks

Task	Procedure	Reference
Enable FTP to create or update ISPF member statistics using the GET or MGET subcommands.	From the client, do one of the following: <ul style="list-style-type: none"> • Specify the ISPFSTATS TRUE statement on FTP.DATA. • Specify the LOCSITE subcommand: LOCSITE ISPFSTATS=TRUE. 	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Table 118. ISPF statistics - Migration tasks (continued)

Task	Procedure	Reference
Enable FTP to create or update ISPF Member statistics using the PUT, MPUT or APPEND subcommands.	From the server, do one of the following: <ul style="list-style-type: none"> Specify the ISPFSTATS TRUE statement on FTP.DATA. Specify the SITE subcommand: SITE ISPFSTATS=TRUE. 	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

User-level FTP server options

In z/OS V1R2 Communications Server, FTP users and system programmers can use FTPS.RC configuration data set to configure user-level options. You can insert SITE and CWD commands in your FTPS.RC file, according to the preferences of each user ID.

Restrictions: Only SITE and CWD subcommands that have valid parameters should be included in your FTPS.RC file.

Migration procedures: The user-level FTP server options function does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 119. User-level FTP server options - Migration task

Task	Procedure	Reference
Customize the FTP server setting for each user.	Create one of the following files: <ul style="list-style-type: none"> tso_prefix.FTPS.RC \$HOME/ftps.rc userid.FTPS.RC <p>Include series of CWD and SITE commands to specify the desired setting for the user with userid.</p> <p>Note: Ensure that the files are readable and that they only include SITE and CWD subcommands that have valid parameters.</p>	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Stream mode restart

z/OS V1R2 Communications Server supports restarting an FTP file transfer when the data transmission mode is STREAM. A few restrictions apply, but in general, stream restarts are supported when the following conditions are met:

- The mode is STREAM.
- The data type is either ASCII, EBCDIC, or Image (binary).
- The file type is SEQ.
- The local file resides in the HFS.

Earlier releases supported restart of FTP file transfer only when the data transmission mode was BLOCK and the data type was EBCDIC.

Restrictions for the FTP server: The following restrictions apply for the FTP server:

- The mode is STREAM.
- The structure must be FILE.
- The file type is SEQ.
- The server file must reside in the HFS.

- If the ASCII to EBCDIC code page for the data connection contains the character <NL>, stream restarts cannot be supported for data type ASCII.

Dependencies for the FTP server: The following dependencies apply for the FTP server:

- The server must use the FTP.DATA statements, LOCSITE, and SITE options that were in effect at the time of the failed data transfer.
- The server must have EXTENSIONS SIZE and EXTENSIONS REST_STREAM coded in FTP.DATA.

Restrictions for the FTP client: The following restrictions apply for the FTP client:

- The mode must be STREAM.
- The structure must be FILE.
- The file type must be SEQ.
- The sunique option must be OFF.
- Only SBCS file transfers are supported.
- When restarting GET, the local file must reside in the HFS.
- When restarting PUT, the remote host must support SIZE for that file.

Dependencies for the FTP client: The following dependency applies for the FTP client:

- The client must re-create the start options, FTP.DATA statements, LOCSITE, and SITE options that were in effect at the time of the failed data transfer.

Migration procedures: The stream mode restart function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 120. Stream mode restart - Migration tasks

Task	Procedure	Reference
Enable the stream restart function in FTP server.	Edit the server FTP.DATA and add EXTENSIONS REST_STREAM AND EXTENSIONS SIZE.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Use the client SRESTART GET and SRESTART PUT subcommands.	Use the help text from the client session, or consult documentation.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Interpret the client messages that result from using SRESTART GET or SRESTART PUT subcommands.	Consult FTP Replies.	<i>z/OS Communications Server: IP and SNA Codes</i>

RFC updates

z/OS V1R2 Communications Server enhances the FTP server and client through RFC 2389 and RFC 2640.

RFC 2389: RFC 2389 — Feature negotiation mechanism for the File Transfer Protocol

- The server recognizes and responds to the FEAT command and the OPTS command.

- The client has a new user command, FEATURE, which sends a FEAT command to the server and displays the response.

Restrictions for RFC 2389: The following restriction applies for RFC 2389:

- Although OPTS is supported, no OPTS command options are currently implemented.

Dependencies for RFC 2389: The following dependency applies for the FTP server:

- The FEAT server response depends on whether the server has EXTENSIONS SIZE, EXTENSIONS UTF8, or EXTENSIONS MDTM encoded in FTP.DATA, and whether the server can locate the UTF-8 conversion table.

Migration procedures for RFC 2389: The RFC 2389 updates do not require any action unless you want to use the FEATURE subcommand. If so, perform the tasks in the following table.

Table 121. RFC 2389 Updates - Migration tasks

Task	Procedure	Reference
Enable RFC 2389.	No action is required.	
Use the client FEATURE subcommand.	Use the help text from the client session, or consult <i>z/OS Communications Server: IP User's Guide and Commands</i> .	<i>z/OS Communications Server: IP User's Guide and Commands</i>
Interpret server response to the FEATURE subcommand.	Consult <i>z/OS Communications Server: IP Messages Volume 1 (EZA)</i> , FTP Replies.	<i>z/OS Communications Server: IP Messages Volume 1 (EZA)</i>

RFC 2640: RFC 2640 — Internationalization of the File Transfer Protocol

- The server recognizes and responds to the LANG command, provided the server's FTP.DATA has coded EXTENSIONS UTF8.
- The server will ignore configuration options to use a specific code page on the control connection when EXTENSIONS UTF8 is coded in FTP.DATA.
- The client has a new user subcommand, LANGUAGE, which sends a LANG command to the server and displays the response. This subcommand is available only if client has EXTENSIONS UTF8 coded in FTP.DATA.
- When EXTENSIONS UTF8 is coded in FTP.DATA, the client will ignore configuration options that affect the code page used on the control connection.

Restrictions for RFC 2640: The following restrictions apply for RFC 2640:

- The client will not send a LANG command to the server if EXTENSIONS UTF8 is not coded in FTP.DATA.
- The client will not send a LANG command to the server if the client is not able to load the UTF-8 translation table at startup.
- The server will not recognize the LANG command if the UTF-8 translation table cannot be loaded at startup.
- The server will not recognize LANG command unless EXTENSIONS UTF8 is coded in FTP.DATA.
- The only language shipped with FTP for z/OS CS is US English.

Dependencies for RFC 2640: The following dependency applies for the FTP client:

- The National Language Resources component of z/OS Language Environment must be installed to get the RFC 2640 functions.

Migration procedures for RFC 2640: The RFC 2640 updates do not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 122. RFC 2640 Updates - Migration tasks

Task	Procedure	Reference
Enable RFC 2640 function in FTP client and server.	Edit the server and client FTP.DATA and add EXTENSIONS UTF8.	<i>z/OS Communications Server: IP Configuration Reference</i>
Remove the configuration options that specify a specific code page on the FTP control connection.	Do the following: <ul style="list-style-type: none"> Edit the server and client FTP.DATA. Remove the CCXLATE and CTRLCONN statements. Remove the TCPXLBIN file from the search order. 	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Verify that the UTF-8 conversion table is installed and available to FTP server and client.	Follow procedures in <i>z/OS C/C++ Programming Guide</i> .	<i>z/OS C/C++ Programming Guide</i>
Use the client LANGUAGE subcommand.	Use the help text from the client session, or consult <i>z/OS Communications Server: IP User's Guide and Commands</i> .	<i>z/OS Communications Server: IP User's Guide and Commands</i>
Interpret server response to the LANGUAGE subcommand.	Consult <i>z/OS Communications Server: IP Messages Volume 1 (EZA)</i> , FTP Replies.	<i>z/OS Communications Server: IP Messages Volume 1 (EZA)</i>
Stop UTF-8 encoding for the control connection for the rest of the login session.	Issue SITE and LOCSITE subcommands to set the control connection code page.	<i>z/OS Communications Server: IP User's Guide and Commands</i>
Override the client's EXTENSIONS UTF8 statement in FTP.DATA.	Use the translate start option to specify a code page for the control connection.	<i>z/OS Communications Server: IP User's Guide and Commands</i>

Native ASCII support

z/OS now allows HFS files to contain ASCII data instead of EBCDIC data. The FTP support has been extended to transfer ASCII files from the HFS, and to store ASCII files into the HFS. This support is part of native ASCII RTL implementation on z/OS of a new tag for HFS files, identifying the contents as binary, ASCII, or EBCDIC.

New messages and new replies may be displayed when a tagged HFS file is transferred between client and server. The messages and replies are informational and they let the client know that a tagged file was transferred and which translation table was used to transfer it.

Restrictions: None.

Migration procedures: The native ASCII support function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 123. Native ASCII support - Migration tasks

Task	Procedure	Reference
Define a data connection translate table with an ASCII file system code page.	Specify the following in either the FTP.DATA client or server data set: SBDDATACONN (ISO8859-1,ISO8859-1)	<i>z/OS Communications Server: IP User's Guide and Commands</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Change the data connection translate table to have an ASCII system code page by using a client subcommand.	Issue LOCSITE SBD=(ISO8859-1,ISO8859-1). Issue SITE SBD=(ISO8859-1,ISO8859-1).	<i>z/OS Communications Server: IP User's Guide and Commands</i>

FTP trace enhancements

FTP provides methods for gathering traces for diagnosis. z/OS V1R2 Communications Server enhances those methods by allowing you to control what is traced. This is accomplished by new options for the server's MODIFY command and new parameters for the client's DEBUG subcommand. Also, a new client DUMP subcommand is added and new FTP.DATA statements are supported.

Prior to this release, tracing was enabled by the MODIFY command and the client's DEBUG subcommand. The client's DEBUG subcommand with an option of 2 activated the general and the extended trace. In this release, DEBUG activates the general trace and the DUMP command activates the extended trace. In z/OS V1R2 Communications Server, tracing can be enabled in several ways:

- You can specify the MODIFY command at the server to enable server tracing.
- You can specify SITE subcommands to enable server tracing.
- You can specify the DEBUG and DUMP subcommand at the client to enable client tracing.
- You can specify the new FTP.DATA statements DEBUG and DUMP to enable both client and server tracing.

Restrictions: None.

Migration procedures: The FTP trace enhancements function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 124. FTP trace enhancements - Migration tasks

Task	Procedure	Reference
Identify where you have MODIFY operator commands for the FTP server trace and change the trace parameters to the new format.	Follow the guidelines that describe the new MODIFY commands parameters that replace the old parameters.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Use the new general tracing parameters and the new extended tracing subcommand.	Replace DEBUG 2 with DEBUG and DUMP subcommands.	<i>z/OS Communications Server: IP User's Guide and Commands</i>

Communications Server for OS/390 V2R10 release summary

This section is divided into two parts: FTP server and FTP client. Descriptions and migration procedures for the FTP functions new in CS for OS/390 V2R10 are provided.

FTP server

Usability enhancements

Recognize new Common INET stack automatically: Prior to CS for OS/390 V2R10, the FTP server would not recognize any Common INET stack started after FTP was started. The operator had to stop and restart FTP to accept connections from the new stack. In CS for OS/390 V2R10, the FTP server will automatically recognize CINET stacks started after FTP is started.

Restrictions: None.

Migration procedures: There are no migration tasks.

Enhanced STAT and LOCSTAT commands: In CS for OS/390 V2R10, the STAT and LOCSTAT commands are enhanced to display additional setting information. Refer to *z/OS Communications Server: IP User's Guide and Commands* for details.

Restrictions: None.

Migration procedures: There are no migration tasks.

Welcome page support: System administrators can now display banners as reply messages (prefixed with 220-, 230-, 250-) to better inform users when they:

- FTP into their server (these replies are prefixed with 220-).
- Log in for both real users and anonymous users (these replies are prefixed with 230-).
- Change into certain directories (these replies are prefixed with 250-).

All of the messages need to be created by the system administrator of the server.

Restrictions: None.

Migration procedures: The welcome page support function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Notes:

1. When specifying parameters in FTP.DATA, the valid file path must be specified and it must point to the existing files.
2. The system administrator must ensure that the files or data sets exist, that they are readable files, and that they include the message to be displayed (the system administrator must write the message). The message files may not be longer than 100 lines in length or they will truncate.

Table 125. Welcome page support - Migration tasks

Task	Procedure	Reference
Display welcome banner replies when client FTPs to the server.	Specify BANNER parameter in FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i>
Display Login Info replies when client logs in as a known user.	Specify LOGINMSG parameter in FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i>
Display Login Info replies when client logs in as an anonymous user.	Specify ANONYMOUSLOGINMSG parameter in FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i>

Table 125. Welcome page support - Migration tasks (continued)

Task	Procedure	Reference
Display Directory Info replies when a known user changes directory into an MVS data set that contains the specified file.	Specify MVSINFO parameter in FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i>
Display Directory Info replies when an anonymous user changes directory into an MVS data set that contains the specified file.	Specify ANONYMOUSMVSINFO parameter in FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i>
Display Directory Info replies when a known user changes directory into an HFS directory that contains the specified file.	Specify HFSINFO parameter in FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i>
Display Directory Info replies when an anonymous user changes directory into an HFS directory that contains the specified file.	Specify ANONYMOUSHFSINFO parameter in FTP.DATA.	<i>z/OS Communications Server: IP Configuration Reference</i>
Create the message file that is being specified in FTP.DATA.	Ensure that the message files are no longer than 100 lines in length to avoid truncation.	<i>z/OS Communications Server: IP Configuration Reference</i>
Enhance content of the banner messages.	<p>The % and metacharacter are expanded. Use one or more of the special character strings of % followed by an alphabetic character. The alphabetical characters are case-sensitive and must be uppercase. The character strings are as follows:</p> <p>%T Local time in some standard form (Thu Nov 15 17:12:42 1990)</p> <p>%C Current working directory</p> <p>%E %E is replaced by the keyword specified by ADMINEMAILADDRESS in FTP.DATA. When ADMINEMAILADDRESS is not specified, it will be replaced by a null value.</p> <p>%R Remote host name</p> <p>%L Local host name</p> <p>%U Username (logged in user). Note: %U is not valid in BANNER data set.</p>	<i>z/OS Communications Server: IP Configuration Reference</i>

Administration enhancements

Request e-mail address as a password for anonymous users: The e-mail address of the client is required whenever ANONYMOUSLEVEL is 3 or greater, and the ANONYMOUS statement specifies no user ID or password, or the ANONYMOUS statement specifies both user ID and password.

Restrictions: The integrity checking done on the e-mail addresses entered by users is rudimentary.

Migration procedures: The request e-mail address as a password for anonymous users function does not require any action unless you want to take advantage of the new function. If so, perform the task in the following table.

Table 126. Request e-mail address as a password for anonymous users - Migration task

Task	Procedure	Reference
Request or require that anonymous users supply e-mail addresses.	Include the following parameters in FTP.DATA: <ul style="list-style-type: none"> • ANONYMOUS • ANONYMOUSLEVEL • EMAILADDRCHECK <p>Note: ANONYMOUSLEVEL must be set to 3 or higher and the directories must be correctly configured. EMAILADDRCHECK determines whether the e-mail address undergoes validation.</p>	<i>z/OS Communications Server: IP Configuration Reference</i>

Extending SMF 118 record for byte transfer count: Two new bytexfer fields are now included in the System Management Facility (SMF) records.

Restrictions: None.

Migration procedures: The extending SMF 118 record for byte transfer count function does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 127. Extending SMF 118 record for byte transfer count - Migration Task

Task	Procedure	Reference
Modify the SMF formatter to read two additional fields at the end of the SMF Record.	There are two new fields to better reflect byte transfer counts for large data transfers: <ul style="list-style-type: none"> • 8-byte long floating-point field (1 byte for the exponent and 7 bytes for the fraction). • 4-byte long unsigned integer for 4-gigabyte counter (incremented once for every 4-gigabytes transferred). 	<i>z/OS Communications Server: IP Configuration Reference</i>

Server anonymous enhancements: New FTP.DATA keywords are supported by the FTP server restricting an anonymous user's access to HFS and MVS data sets and files.

A keyword introduced by an APAR, anonymouslevel, will indicate the degree to which anonymous login users are restricted.

Anonymouslevel 1

Anonymous logins are affected only by the ANONYMOUS keyword. APAR PQ28980 function is excluded.

Anonymouslevel 2

Introduced with APAR PQ28980. When anonymouslevel is set to 2 and the STARTDIRECTORY statement specifies HFS, the UNIX call chroot() will be used to set the anonymous user's root directory to the anonymous user's home directory. A umask of 777 will be used for all files and directories created by anonymous users.

Anonymouslevel 3

New for this release. Like anonymouslevel 2, the UNIX call chroot() will be used to establish the anonymous user's root directory when the

STARTDIRECTORY statement specifies HFS. The USER command will be disabled for switches to and from anonymous user IDs. Additionally, these new FTP.DATA keywords will affect how the anonymous user can access and create files:

- ANONYMOUSFILETYPESEQ, ANONYMOUSFILETYPEJES, and ANONYMOUSFILETYPESQL will control whether the anonymous user can use the SITE FILETYPE=SEQ, SITE FILETYPE=JES, or SITE FILETYPE=SQL commands, respectively.
- ANONYMOUSFILEACCESS will control whether the anonymous user has access to the HFS, to MVS files, or both.
- ANONYMOUSHFSFILEMODE sets the mode bits, or access permissions, of HFS files written by anonymous users.
- ANONYMOUSHFSDIRMODE sets the mode bits, or access permissions, of HFS directories created by anonymous users.

Restrictions: The following restrictions apply:

- Anonymouslevel 2 is provided for users of APAR PQ28980 who do not wish to migrate to anonymouslevel 3. IBM does not recommend setting ANONYMOUSLEVEL 2 in other circumstances. The preferred method is to use ANONYMOUSLEVEL 3.
- If you are migrating from APAR PQ28980, you may not require the sample exit routine provided with that APAR. Review your exit routine requirements in light of the new FTP.DATA keywords available to ANONYMOUSLEVEL 3 users.
- If you set ANONYMOUSLEVEL to 3, anonymous users will be required to enter an e-mail address as password in cases where no password was formerly required. Any automation that uses an anonymous FTP client to the CS for OS/390 FTP server may need to be updated to provide this.

What this change affects:

- FTP server customization
- HFS directory structure

Migration procedures: The server anonymous enhancements function does not require any action if you are satisfied with the CS for OS/390 V2R5 style of anonymous user's access to HFS and MVS resources. Optionally, define ANONYMOUSLEVEL 1 explicitly in FTP.DATA. This is the default value of ANONYMOUSLEVEL. It indicates that the anonymous user's access to HFS and MVS resources remains the same as was supported by CS for OS/390 V2R5.

If you have applied APAR PQ28980 and you are satisfied with that support, ensure ANONYMOUSLEVEL 2 is defined in FTP.DATA. This indicates the anonymous user's access to HFS and MVS resources is as supported by CS for OS/390 V2R5. Maintain the anonymous root directory structure defined by APAR PQ28980. Furthermore, if you are using APAR PQ28980, you can perform the tasks in the following table.

Table 128. Server anonymous enhancements using APAR PQ28980 - Migration tasks

Task	Procedure	Reference
Decide whether to migrate from ANONYMOUSLEVEL 2 to ANONYMOUSLEVEL 3.	If you choose to remain at ANONYMOUSLEVEL 2, maintain the exit routine and HFS anonymous root directory structure defined by the APAR.	<i>z/OS Communications Server: IP Configuration Reference</i>

Table 128. Server anonymous enhancements using APAR PQ28980 - Migration tasks (continued)

Task	Procedure	Reference
If you are migrating to ANONYMOUSLEVEL 3, review your security exit requirements in light of the new keywords available to ANONYMOUSLEVEL 3 users.	You may find that you do not need the exit routine. Revise or eliminate the exit routine as needed.	<i>z/OS Communications Server: IP Configuration Reference</i>
If you are migrating to ANONYMOUSLEVEL 3, define keywords.	Define ANONYMOUSLEVEL 3 in the server's FTP.DATA. Define other keywords in the server's FTP.DATA as needed: ANONYMOUSFILETYPESEQ ANONYMOUSFILETYPEJES ANONYMOUSFILETYPESQL ANONYMOUSFILEACCESS ANONYMOUSHFSFILEMODE ANONYMOUSHFSDIRMODE	<i>z/OS Communications Server: IP Configuration Reference</i>

If you have *not* applied APAR PQ28980, you can perform the tasks in the following table.

Table 129. Server anonymous enhancements when not using APAR PQ28980 - Migration tasks

Task	Procedure	Reference
Define keywords for enhanced anonymous support.	Define ANONYMOUSLEVEL 3 in the server's FTP.DATA. Define other keywords in the server's FTP.DATA as needed: ANONYMOUSFILETYPESEQ ANONYMOUSFILETYPEJES ANONYMOUSFILETYPESQL ANONYMOUSFILEACCESS ANONYMOUSHFSFILEMODE ANONYMOUSHFSDIRMODE	<i>z/OS Communications Server: IP Configuration Reference</i>
Establish an HFS anonymous root directory and subtree as defined in <i>z/OS Communications Server: IP Configuration Reference</i> .	Optionally, use the shell script, ftpandir.scp, that is provided in /usr/lpp/tcpip/samples. You do not need to use the shell script if you prefer to manually set up the directory structure.	<i>z/OS Communications Server: IP Configuration Reference</i>

Functional and compatibility enhancements

Load module transfer: Load module transfer is an enhancement that allows you to use the FTP client and server to transfer MVS load modules between CS for OS/390 V2R10 and above systems.

When an FTP transfer is attempted on a file that is an MVS load module, special processing is invoked. No user action or input is required. If the special processing fails, the file transfer may continue but the transferred load modules will not be executable on the target system. For example, this type of failure would occur if there were mismatched versions for the client and server. Refer to *z/OS Communications Server: IP User's Guide and Commands* for details.

Restrictions: The following restrictions apply:

- Only CS for OS/390 V2R10 or later to CS for OS/390 V2R10 or later transfers are valid; transfers between back levels of FTP client or server, or between any third party FTP servers or clients, will not be executable on the target system.

- The IEBCOPY system utility must be in the linked list of the client and the server.
- The FTP client must be started in one of these environments:
 - TSO terminal session
 - TSO background
 - TSO batch
 - TSO REXX
 - UNIX System Services terminal session

Note: REXX running under UNIX System Services is not supported.

- Load modules cannot be renamed on transfer.
- Load modules must be transferred between the same type of load library data sets (for example, PDS to PDS or PDSE to PDSE).

Migration procedures: There are no migration tasks.

Extensions to FTP: SIZE and MDTM: SIZE and MDTM are new commands proposed by an FTP extension draft RFC. SIZE returns the number of bytes that would be transferred to the client if the client were to get the file from the server. MDTM returns the time the file was last modified. These commands are now supported by the FTP server. Since these commands are not part of RFC 959, the FTP server will support them only if the system administrator has defined FTP.DATA statements to enable them.

Restrictions: The following restrictions apply:

- By default, support for MDTM and SIZE is not enabled.
- MDTM is supported only for HFS data sets.
- SIZE and MDTM are supported for filetype SEQ only.
- SIZE is not supported for all file types that FTP is able to transfer. SIZE is supported for HFS files only, and only when mode is stream, file structure is FILE, and data transfer type is IMAGE.

Migration procedures: The extensions to FTP: SIZE and MDTM function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 130. Extensions to FTP: SIZE and MDTM function - Migration tasks

Task	Procedure	Reference
Determine whether your server should support SIZE and MDTM. Certain FTP clients, such as Web browsers, may use SIZE and MDTM commands even though they are not defined in the FTP RFC 959.	If so, perform the next two tasks (optionally).	<i>Extensions to FTP draft document</i>
Enable the FTP server to support the SIZE command.	In the server FTP.DATA, define EXTENSIONS SIZE.	<i>z/OS Communications Server: IP Configuration Reference</i>
Enable the FTP server to support the MDTM command.	In the server FTP.DATA, define EXTENSIONS MDTM.	<i>z/OS Communications Server: IP Configuration Reference</i>

Transfer MVS data sets with FTP URL: In CS for OS/390 V2R10, FTP clients can code an FTP URL to transfer an MVS data set. You may enter the FTP URL directly into a Web browser, or you may encode it into an HTML script.

The FTP System Administrator enables this support by defining an MVSURLKEY string. Users encode the defined MVSURLKEY in the FTP URL to indicate that the string following is an MVS data set name.

Restrictions: None.

Incompatibilities: Be aware of the following:

- Select the MVSURLKEY judiciously to avoid metacharacters that FTP clients may interpret instead of passing on to the FTP server.
- When selecting a name for a key, WebSphere users should choose a name that matches the WebSphere configuration directive for encoding MVS data set URLs.
- If the MVSURLKEY happens to match the name of an HFS root subdirectory, that directory will be closed to FTP transfers.

Migration procedures: The transfer MVS data sets with FTP URL function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 131. Transfer MVS data sets with FTP URL - Migration tasks

Task	Procedure	Reference
Provide FTP clients the ability to encode an MVS data set name in an FTP URL.	Do the following: <ul style="list-style-type: none"> • Select an MVSURLKEY according to the requirements defined in <i>z/OS Communications Server: IP Configuration Reference</i>. • Define the MVSURLKEY keyword in the server's FTP.DATA. • Inform your FTP clients that the MVSURLKEY is available for use in FTP URLs. HTML script writers and Web browser users are potential users of FTP URLs. 	<i>z/OS Communications Server: IP Configuration Reference</i>

FTP SITE and LOCSITE allocation keywords: CS for OS/390 V2R10 introduces new and changed keywords to the FTP client SITE and LOCSITE commands to allow a data set to be allocated across multiple volumes. There are new FTP.DATA statements to allow the keywords.

The keywords are:

VCOUNT

New. VCOUNT sets the volume count for new allocations.

UCOUNT

New. UCOUNT sets the unit count for new allocations.

VOLUME

Changed. VOLUME sets volume serial number for new allocations, or a list of volume serial numbers for new allocations. Existing code supports specifying a single volume serial number. The enhancement is to allow more than one volume serial number to be specified.

Restrictions: Be aware of the following:

- The FTP server and client do not attempt to diagnose incompatible UCOUNT, VCOUNT, and VOLUME combinations while processing SITE or LOCSITE commands, nor while processing FTP.DATA statements. It is up to the user to understand the implications of overriding system defaults for UCOUNT, VCOUNT, and VOLUME.
- The new keywords are intended for non-SMS environments, because SMS storage classes can override whatever the user specifies for VCOUNT, UCOUNT, and VOLUME.

Migration procedures: The FTP SITE and LOCSITE allocation keywords function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 132. FTP SITE and LOCSITE allocation keywords - Migration tasks

Task	Procedure	Reference
Use the new keywords for server/remote allocations.	Do one of the following: <ul style="list-style-type: none"> • From the client, issue a SITE command specifying the new keywords. For the duration of the client session, the specified SITE values will affect MVS allocations on the remote host. • In the server FTP.DATA data set, define UCOUNT, VCOUNT, and VOLUME. These values will be applied to all MVS allocations on the server, for all clients. • Clients can query the current settings with a STAT command. Clients can revert to system defaults or override the current settings using a SITE command. 	<i>z/OS Communications Server: IP Configuration Reference</i>
Use the new keywords for client/local allocations.	Do one of the following: <ul style="list-style-type: none"> • From the client, issue a LOCSITE command specifying the new keywords. For the duration of the client session, the specified LOCSITE values will affect MVS allocations on the remote host. • In the client FTP.DATA data set, define UCOUNT, VCOUNT, and VOLUME. These values will be applied to all MVS allocations on the client, for all clients. • Clients can query the current settings with a LOCSTAT command. Clients can revert to system defaults or override the current settings using a LOCSITE command. 	<i>z/OS Communications Server: IP Configuration Reference</i>

FTP JES: The FTP/JES interface is enhanced in CS for OS/390 V2R10 to provide three new SITE keywords to allow users to select the userid (keyword JESOWNER), jobname (JESJOBNAME), and type (JESSTATUS) of output to receive. This enhancement removes the restriction of FTP clients only being able to receive jobs that match their userid plus one character.

An additional FTP.DATA keyword, JESINTERFACELEVEL, is added to allow installations to select JESINTERFACELEVEL 2. Installations that want to continue using the previous version of the interface can either leave the JESINTERFACELEVEL keyword out of their FTP.DATA file or code the default JESINTERFACELEVEL 1.

For those installations that want to take advantage of the new interface, security measures should be put in place to ensure that FTP clients can only get to JES output for which they are authorized. The Security Access Facilities (SAF or RACF) resource classes used by the new interfaces are the JESSPOOL and SDSF resource classes. These classes are documented in the *z/OS JES2 Initialization*

and Tuning Guide and the z/OS SDSF Operation and Customization. Those installations currently configured for these two SAF resource classes have no migration to the enhanced FTP JES interface.

Restrictions: This enhanced function is available when the server FTP.DATA specifies JESINTERFACELEVEL 2. Be aware of the following:

- If you want to use the new FTP JES support (specifying JESINTERFACELEVEL 2) and you are running JES3, you must be running at least JES3 V3R5.
- Regardless of what release you are running, you must have the appropriate APARs installed. For JES2, the APAR is OW41734. For JES3, the APARs are OW36022, OW34753 and OW35435.
- The Security Access Facilities (SAF) resource must be in place. (The SAF resources are those used by JES and SDSF.)

Migration procedures: The FTP JES function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 133. FTP JES - Migration tasks

Task	Procedure	Reference
Determine whether FTP clients should have more access to JES resources in an installation.	Update server FTP.DATA to specify JESINTERFACELEVEL 2 if enhanced access is desired.	<i>z/OS Communications Server: IP Configuration Reference</i>
Ensure security is in place for enhanced access.	Update SAF resources.	<i>z/OS Communications Server: IP Configuration Reference, z/OS Communications Server: IP Configuration Guide, z/OS JES2 Initialization and Tuning Reference, and z/OS SDSF Operation and Customization</i>
Inform end users (FTP clients) who wish to take advantage of the enhanced function of the SITE JESOWNER, JESJOBNAME, and JESSTATUS keywords.	Per installation procedures.	<i>z/OS Communications Server: IP User's Guide and Commands</i>

User exit enhancements

user exits: The user written exit, FTCHKCMD, is enhanced to support additional parameters that allow for exits to be written with the following abilities:

- Control user execution of FTP subcommands
- Accept parameters from non-IBM FTP clients
- Modify the command parameter string

A new FTCHKCMD sample is provided in SEZAINST(FTCHKCMD) and SEZAINST(FTCHKCM1). Another sample is provided in SEZAINST(FTCHKCM2).

The SEZAINST(FTPOSTPR) exit was also added in CS for OS/390 V2R10. It is invoked when the FTP commands RETR, STOR, STOU, APPE, DELE, and RNT0 complete. This new exit allows for user post processing of file transfers regardless of their success or failure. A sample FTPOSTPR is provided in *hlq*.SEZAINST.

Restrictions: None.

Migration procedures: The user exit enhancements function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 134. User exit enhancements - Migration tasks

Task	Procedure	Reference
Modify existing exits.	Use the new FTCHKCMD parameters.	<i>z/OS Communications Server: IP Configuration Reference</i>
Ensure proper authorization.	The user exit load modules must be placed in an APF-authorized library to which the FTP server has access by STEPLIB, linklist, or LPA. Also, the authorization state (JSCBAUTH) must be the same after exiting from the user exit as it was upon entry. If a user exit is not found, processing proceeds as though a return code of 0 was received from the user exit call.	<i>z/OS Communications Server: IP Configuration Reference</i>
Perform user post processing on FTP file transfer commands.	Write and install the new FTPOSTPR exit.	<i>z/OS Communications Server: IP Configuration Reference</i>

FTP client

Usability enhancements

Enhanced STAT/LOCSTAT commands: See “Enhanced STAT and LOCSTAT commands” on page 192 for both the client and server migration considerations.

FTP batch jobs comments: In CS for OS/390 V2R10, you can now add or insert comments in the input sections of the batch files for FTP. Refer to the syntax details in *z/OS Communications Server: IP User's Guide and Commands* and also to the sample FTP batch job file, *hlq.SEZAINST(IVPFTP)*.

Restrictions: None.

Migration procedures: There are no migration tasks.

Administration enhancements

Extending SMF 118 record for byte transfer count: See “Extending SMF 118 record for byte transfer count” on page 194 for both the client and server migration considerations.

Functional and compatibility enhancements

Load module transfer: See “Load module transfer” on page 196 for both the client and server migration considerations.

DDname support: This enhancement allows the FTP client to use a DDname allocated by the user for a local data set.

Restrictions: The following restrictions apply:

- DDnames can only be specified at the FTP client, and only for local files (server files cannot be specified by DDname).
- To use DDname support, the client's local working directory cannot be in the HFS.

- When PUTting a local file specified by DDname, the user must provide the remote file name.

Migration procedures: The DDname support function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 135. DDname support - Migration tasks

Task	Procedure	Reference
Specify a DD name for transfer.	Allocate a local file to a specific DDname.	<i>z/OS Communications Server: IP User's Guide and Commands</i>
Use the get and put commands to refer to a file allocated to a specific DDNAME.	Use the syntax //DD:DDNAME in the FTP client.	<i>z/OS Communications Server: IP User's Guide and Commands</i>

FTP SITE and LOCSITE allocation keywords: See “FTP SITE and LOCSITE allocation keywords” on page 198 for both the client and server migration considerations.

FTP JES: See “FTP JES” on page 199 for both the client and server migration considerations.

Chapter 10. Migrating the Telnet server and client

Telnet is a terminal emulation protocol that allows you to log on to a remote host as though you were directly attached to that host.

z/OS CS Telnet consists of client and server components. Refer to *z/OS Communications Server: IP User's Guide and Commands* for guidance on using the client component.

The server component includes an updated version of the Telnet server available in previous releases and a z/OS UNIX Telnet server that lets hosts in an IP network log on to the z/OS shell environment directly, without going through TSO. The z/OS UNIX Telnet server supports AIX® and UNIX full-screen applications such as the vi editor, so that AIX and UNIX users can use familiar Telnet commands. The z/OS UNIX Telnet server runs in both line mode and raw mode, but does not support TN3270 or TN3270E, as Telnet does. Refer to *z/OS Communications Server: IP Configuration Guide* for more information about either Telnet server.

The z/OS CS Telnet server runs in the TCP/IP address space. It is a part of TCP/IP. It does not have its own startup procedure; it is started when TCP/IP is started if the necessary Telnet statements are in the profile. The Telnet server communicates with VTAM using either LU0 or LU2 for terminal support and LU1 or LU3 for printer support.

This chapter contains new and changed Telnet interfaces, including:

- “TELNETGLOBALS information block” on page 204
- “TELNETPARMS information block” on page 205
- “BEGINVTAM information block” on page 206
- “UNIX Telnet server (otelnetd) configuration” on page 209
- “Telnet operator commands” on page 209

This chapter also contains the following for Telnet:

- “z/OS V1R4 Communications Server release summary” on page 211
- “z/OS V1R2 Communications Server release summary” on page 216
- “Communications Server for OS/390 V2R10 release summary” on page 222

New and changed interfaces for Telnet

Telnet PROFILE.TCPIP configuration file

During initialization of the TCP/IP address space, system operation and configuration parameters are read from a configuration PROFILE data set. The PROFILE data set is used to configure Telnet to accept or reject connection requests. You can update the PROFILE data set to change or add statements to support new functions, or to change or add usage rules.

This section includes tables with the descriptions of the new and changed Telnet PROFILE.TCPIP configuration files. Refer to *z/OS Communications Server: IP Configuration Reference* for complete information on configuration files and the PROFILE statement.

TELNETGLOBALS information block

The TELNETGLOBALS information block is a Telnet configuration block used to provide definitions that apply to all Telnet ports. It was introduced in CS for OS/390 V2R10.

Table 136. PROFILE.TCPIP — TELNETGLOBAL configuration file (Telnet)

Statement or parm	Description	Status
KEYRING	Allows designation of the key ring to be used for all SECUREREPORTs. This KEYRING specification overrides any KEYRING statements specified in the TELNETPARMS block.	New in CS for OS/390 V2R10
CRLLDAPSERVER/ ENDCRLLDAPSERVER	Allows designation of the LDAP server address and port that will be used for certificate revocation list (CRL) checks.	New in CS for OS/390 V2R10
CLIENTAUTH	Used to specify client authentication.	New in CS for OS/390 V2R10
DEBUG	Allows SUMMARY or DETAIL debug messages to be displayed on console or job log. In z/OS CS V1R2, TRACE option is added.	New in CS for OS/390 V2R10
ENCRYPTION	Turns on encryption debugging code.	New in CS for OS/390 V2R10
INACTIVE KEEPINACTIVE PRTINACTIVE SCANINTERVAL TIMEMARK SSLTIMEOUT CODEPAGE TN3270E (NOTN3270E) SIMCLIENTLU (NOSIMCLIENTLU) EXPRESSLOGON (NOEXPRESSLOGON) SNAEXT (NOSNAEXT) SMFINIT (SMFTERM) LUSESSIONPEND (NOLUSESSIONPEND) MSG07 (NOMSG07) FULLDATATRACE (NOFULLDATATRACE)	These new or existing Telnet parameters can now be specified in TELNETGLOBALS block.	New in z/OS CS V1R2
BinaryLinemode (NoBinaryLinemode) SGA (NOSGA (synonym for DisableSGA)) MaxReceive MaxVTAMsendQ MaxReqSess OldSolicitor (NoOldSolicitor) SingleATTN (NoSingleATTN) TKOspecLU (NoTKO) TKOspecLUrecon (NoTKO) TelnetDevice DropAssocPrinter (NoDropAssocPrinter) SequentialLU (NoSequentialLU) KeepLU (NoKeepLU)	These new or existing Telnet parameters can now be specified in TELNETGLOBALS block.	New in z/OS CS V1R4

TELNETPARMS information block

Table 137. PROFILE.TCPIP — TELNETPARMS configuration file (Telnet)

Statement or parm	Description	Status
CONNTYPE	Allows you to specify whether or not your connection will use SSL protocols.	New in CS for OS/390 V2R10
DEBUG	Allows SUMMARY or DETAIL debug messages to be displayed on console or job log. In z/OS CS V1R2, TRACE option is added.	New in CS for OS/390 V2R10; changed in z/OS CS V1R2
EXPRESSLOGON (NOEXPRESSLOGON)	Controls activation of Express Logon function.	New in z/OS CS V1R2 and APARed back to CS for OS/390 V2R10
KEEPINACTIVE	Statement to define the inactivity timeout for connections with open ACBs while there is no active session with an application.	New in CS for OS/390 V2R10
KEYRING	Changed to support SAF keyring type.	Changed in CS for OS/390 V2R10
NoBinaryLinemode NoSGA (SGA) NoOldSolicitor NoSingleATTN NoTKO NoDBCstransform NoDBCstrace TelnetDevice DropAssocPrinter (NoDropAssocPrinter) SequentialLU (NoSequentialLU) KeepLU (NoKeepLU)	These new or existing Telnet parameters can now be specified in TELNETPARMS block.	New in z/OS CS V1R4
SCANINTERVAL / TIMEMARK	<p>Allows customization of TIMEMARK. In V2R10, SCANINTERVAL/TIMEMARK default is increased from 120/600 seconds to 1800/10800 seconds to avoid network flooding of Timemarks during periods of low activity. If you were using pre-V2R10 default values and still want those old values, Scaninterval/Timemark must be coded.</p> <p>Prior to z/OS CS V1R2, specifying 0 for TIMEMARK or SCANINTERVAL would result in the default value. This was not consistent with other timers (for other timers, specifying 0 would result in turning off the timer). Therefore, in z/OS CS V1R2 and later, it is not possible to specify 0 for TIMEMARK or SCANINTERVAL. If you coded 0 in previous releases for the SCANINTERVAL or TIMEMARK value, you must change this to a valid value. The valid range for TIMEMARK and SCANINTERVAL is from 1-99999999.</p>	Changed in CS for OS/390 V2R10 and z/OS CS V1R2

Table 137. PROFILE.TCPIP — TELNETPARMS configuration file (Telnet) (continued)

Statement or parm	Description	Status
SIMCLIENTLU	Allows incoming TN3270E client requests for Terminal LUs to function the way TN3270 client requests are processed by deferring selection of LUs until after application selection.	New in CS for OS/390 V2R10
SMFINIT	Allows coding of STD to represent the IBM standard number 20 for logging on. Changed in z/OS CS V1R2 to configure the Telnet server to write the new SMF type 119 records.	Changed in z/OS CS V1R2
SMFTERM	Allows coding of STD to represent the IBM standard number 21 for logging off. Changed in z/OS CS V1R2 to configure the Telnet server to write the new SMF type 119 records.	Changed in z/OS CS V1R2
SNAEXT (NOSNAEXT)	Controls the Telnet negotiation begun by the server. The default is SNAExt and it specifies that all TN3270E connection negotiations will permit negotiation of the Contention Resolution and SNA Sense Function of the TN3270E Functional Extensions. NoSNAExt specifies that all connection negotiations will exclude the Contention Resolution and SNA Sense function of the TN3270E Functional Extensions.	New in z/OS CS V1R2
TKOSPECLURECON	Like TKOSPECLU, it allows the setting of time for takeover function to wait to see if original connection is still active. If it is not active, the new connection request will take over the original connection and session.	New in CS for OS/390 V2R10
	In CS for OS/390 V2R10, a new KeepOnTmReset parameter is added. If KeepOnTmReset is specified and a RESET is received by Telnet after the Timemark has been sent, Telnet will keep the session.	Changed in CS for OS/390 V2R10
TRANSFORM	Allowed a vendor transform load module to be attached by Telnet.	Removed in V2R10; use DBCSTRANSFORM.

BEGINVTAM information block

Table 138 includes the PROFILE.TCPIP statements for the BEGINVTAM information block.

Table 138. PROFILE.TCPIP — BEGINVTAM configuration file (Telnet)

Statement or parm	Description	Status
ALLOWAPPL	New LUG parameter allows an LUGROUP name to be specified.	Changed in CS for OS/390 V2R10
DEFAULTAPPL	Changed to now allow the APPL name to be specified as the Network Qualified Name. Also, LOGAPPL, FIRSTONLY, and DEFONLY keywords added to allow clients to request a session with a PLU and wait for the PLU to become active.	Changed in CS for OS/390 V2R10
DEFAULTLUSSPEC / ENDDEFAULTLUSSPEC statement block	New statement block to define the pool of LUs to be used as defaults when a client attempts a connect for a specific LU, and the connection is not mapped to any specific or generic LU group.	New in CS for OS/390 V2R10

Table 138. PROFILE.TCPIP — BEGINVTAM configuration file (Telnet) (continued)

Statement or parm	Description	Status
DEFAULTPRT / ENDDEFAULTPRT statement block	New statement block to define the pool of LUs to be used as defaults when a client attempts a generic connect for a PRT LU and the connection is not mapped to any generic PRTGRP.	New in CS for OS/390 V2R10
DEFAULTPRTSPEC / ENDDEFAULTPRTSPEC statement block	New statement block to define the pool of LUs to be used as defaults when a client attempts a connect for a specific PRT LU, and the specific PRT LU and the connection are not mapped to any specific or generic PRT group.	New in CS for OS/390 V2R10
LINEMODEAPPL 	LOGAPPL, FIRSTONLY, and DEFONLY keywords added to allow clients to request a session with a PLU and wait for the PLU to become active.	New in CS for OS/390 V2R10
LUGROUP 	In z/OS CS V1R4, enhanced to include EXIT option and capacity check.	Changed in z/OS CS V1R4
LUMAP 	CS for OS/390 V2R10 enhanced LUMAP as follows: <ul style="list-style-type: none"> • New keyword KEEPOPEN specifies that the associated LUs are subject to KEEPOPEN processing mode. The LU stays assigned to the connection and the ACB stays open when the session LOGON fails or a session is terminated normally. • New keyword DEFAPPL specifies the initial application to which Telnet will connect. LOGAPPL, FIRSTONLY, and DEFONLY keywords added to allow clients to request a session with a PLU and wait for the PLU to become active. • Multiple LUMAP statements now allowed for a single client identifier. 	Changed in CS for OS/390 V2R10
 	Enhanced to include new QINIT and PMAP options.	Changed in z/OS CS V1R4

Table 138. PROFILE.TCPIP — BEGINVTAM configuration file (Telnet) (continued)

Statement or parm	Description	Status
PARMSGROUP statement block	<p>New parameter block added within the BEGINVTAM block to define parameters that should apply to individual connections. PARMSGROUP block can contain the following:</p> <p>CONNTYPE ENCRYPT (ENDENCRYPT) CLIENTAUTH DEBUG INACTIVE KEEPINACTIVE PRTINACTIVE SCANINTERVAL TIMEMARK SSLTIMEOUT CODEPAGE TN3270E (NOTN3270E) SIMCLIENTLU (NOSIMCLIENTLU) EXPRESSLOGON (NOEXPRESSLOGON) SNAEXT (NOSNAEXT) SMFINIT (SMFTERM) LUSESSIONPEND (NOLUSESSIONPEND) MSG07 (NOMSG07) FULLDATATRACE (NOFULLDATATRACE)</p>	<p>CONNTYPE, ENCRYPT, CLIENTAUTH, and DEBUG were new to PARMSGROUP in CS for OS/390 V2R10. The other parameter statements were new to PARMSGROUP in z/OS CS V1R2.</p>
	<p>PARMSGROUP block can also contain the following entries in z/OS CS V1R4:</p> <p>BinaryLinemode (NoBinaryLinemode) SGA (NOSGA (synonym for DisableSGA)) MaxReceive MaxVTAMsendQ MaxReqSess OldSolicitor (NoOldSolicitor) SingleATTN (NoSingleATTN) TKOspecLU (NoTKO) TKOspecLUrecon (NoTKO) DBCStrtransform (NoDBCStrtransform) DBCStrace (NoDBCStrace) TelnetDevice DropAssocPrinter (NoDropAssocPrinter) SequentialLU (NoSequentialLU) KeepLU (NoKeepLU)</p>	<p>New in z/OS CS V1R4</p>
PARMSMAP statement	<p>New statement to associate a PARMSGROUP block with a client identifier.</p>	<p>New in CS for OS/390 V2R10</p>
PTRDEFAULTAPPL	<p>New mapping statement. It is the same as DEFAULTAPPL except it is for printer connections.</p>	<p>New in z/OS CS V1R4</p>
PRTGROUP	<p>In z/OS CS V1R4, enhanced to include EXIT option and capacity.</p>	<p>Changed in z/OS CS V1R4</p>
PRTMAP	<p>In z/OS CS V1R4, enhanced as follows:</p> <ul style="list-style-type: none"> • QINIT and PMAP options are now included. • New keyword DEFAPPL specifies the initial application to which Telnet will connect. LOGAPPL, FIRSTONLY, and DEFONLY keywords added to allow clients to request a session with a PLU and wait for the PLU to become active. • Multiple LUMAP statements now allowed for a single client identifier. 	<p>Changed in z/OS CS V1R4</p>

Table 138. PROFILE.TCPIP — BEGINVTAM configuration file (Telnet) (continued)

Statement or parm	Description	Status
RESTRICTAPPL	A new LUG option on the USER parameter allows an LUGROUP name to be specified.	Changed in CS for OS/390 V2R10
	New parameter, CERTAUTH, is added to specify the use of USERID obtained from the client X.509 certificate or from Express Logon Feature.	Changed in z/OS CS for V1R2

UNIX Telnet server (otelnetsd) configuration

Table 139 includes the new and changed Telnet configuration. Refer to *z/OS Communications Server: IP Configuration Guide* for complete information on Telnet configuration.

Table 139. New or changed Telnet configuration

Parameter	Description	Status
-a authmode	Specifies authentication mode.	New in z/OS CS V1R2
-D login	otelnetsd will write a concise summary of login and logout activity to the syslog facility "auth".	New in CS for OS/390 V2R10
-D authentication	Turns on authentication debugging code.	New in z/OS CS V1R2
-D encryption	Turns on encryption debugging code	New in z/OS CS V1R2
-T terminfo_value	otelnetsd will set the TERMINFO environment variable to the specified value prior to searching for the terminfo definition for the terminal type specified by the Telnet client. This facility should be used if the administration has configured installation-defined terminfo definitions.	New in CS for OS/390 V2R10
-X authtype	Disables authentication type.	New in z/OS CS V1R2

Telnet operator commands

Table 140 includes the descriptions of the new and changed Telnet operator commands. Refer to *z/OS Communications Server: IP User's Guide and Commands* for complete information on operator commands.

Table 140. New or changed Telnet operator commands

Command	Description	Status
D TCPIP,,TELNET,APPL	Displays information about what applications are being used, how many users are actively using each one, and whether the application is restricted (RESTRICTAPPL) or allowed (ALLOWAPPL). In V2R10, display is enhanced to show LUGROUP information. In z/OS CS V1R4, syntax is obsolete but accepted.	Changed in CS for OS/390 V2R10
D TCPIP,,TELNET,CLIENTID	Displays information about client identifiers defined in the Telnet profile, such as objects mapped and number of active connections.	New in z/OS CS V1R2

Table 140. New or changed Telnet operator commands (continued)

Command	Description	Status
D TCPIP,,TELNET,CONNECTION	<p>Displays information that allows a high-level view of what connections exist and what they are being used for. This command can also take a complete look at one connection.</p> <p>In CS for OS/390 V2R10, display is extended to display the connection type in effect for this connection. If the connection is mapped to a PARMSGROUP, the PARMSGROUP name will also be displayed.</p> <p>Also in CS for OS/390 V2R10, display is extended to include new netid field to the APPLID, add new lines for the LOGAPPL and DEFAULTAPPL information, and indicate when the LU is a KEEPOPEN LU.</p>	Changed in CS for OS/390 V2R10
D TCPIP,,TELNET,DEFAULTS	<p>Displays information to allow verification that the profile information for the DEFAULTLUS, LINEMODEAPPL, USSTCP, and INTERPTCP statements is correct and to understand what was specified in previous profiles when the actual file may no longer be available.</p> <p>In CS for OS/390 V2R10, the display now contains additional information indicating the NETID for a DEFAULTAPPL or LINEMODEAPPL when a Network Qualified Appl name is specified on the DEFAULTAPPL statement or LINEMODEAPPL statement.</p> <p>In z/OS CS V1R4, syntax is obsolete but accepted.</p>	Changed in CS for OS/390 V2R10
D TCPIP,,TELNET,LUGROUP	<p>Displays information about what LUGROUPS and PRTGROUPS are being used, the number of LUs that are defined for each one, and how many of those LUs are already in use.</p> <p>In CS for OS/390 V2R10, display is enhanced to display default specific LU group, default PRT group, and default specific PRT group.</p> <p>In z/OS CS V1R4, syntax is obsolete but accepted.</p>	Changed in CS for OS/390 V2R10
D TCPIP,,TELNET,LUMAP	<p>Displays information about what LUMAPs and PRTMAPs are defined.</p> <p>In CS for OS/390 V2R10, display is changed to consolidate the heading for TYPE, SPEC and a new flag for KEEPOPEN. LOGAPPL name is added, including the netid.</p> <p>In z/OS CS V1R4, syntax is obsolete but accepted.</p>	Changed in CS for OS/390 V2R10
D TCPIP,,TELNET,OBJECT	<p>Displays information about objects defined in the Telnet profile, such as client identifiers mapped and number of active connections.</p>	New in z/OS CS V1R2
D TCPIP,,TELNET,PARMSGROUP	<p>New option to display the connection type, client authentication and encryption support for a parameter group.</p> <p>In z/OS CS V1R4, syntax is obsolete but accepted.</p>	New in CS for OS/390 V2R10

Table 140. New or changed Telnet operator commands (continued)

Command	Description	Status
D TCPIP,,TELNET,PARMSMAP	New option to display the mapping of parameter group names to port or IP address or hostname group. In z/OS CS V1R4, syntax is obsolete but accepted.	New in CS for OS/390 V2R10
D TCPIP,,TELNET,PROFILE	Displays information about what profile-wide options are in effect for each profile, which profiles are still being used, and how many users are on each profile. In CS for OS/390 V2R10, display is enhanced to: <ul style="list-style-type: none"> • Support new options, SUMMARY and DETAIL, to indicate how much information should be displayed. • Show a new profile options flag to indicate whether the SIMCLIENTLU profile statement was specified. • Display CRLLDAPSERVER information. • Display CONNTYPE information. In z/OS CS V1R2, detail display shows all parameter values. The parameters are organized by function.	Changed in CS for OS/390 V2R10 and z/OS CS V1R2
D TCPIP,,TELNET,WHEREUSED	In CS for OS/390 V2R10, display is extended to support PARMSGROUP names. In addition, the display now contains additional information indicating the NETID for a DEFAULTAPPL or LINEMODEAPPL when a Network Qualified Appl name is specified on the DEFAULTAPPL statement or LINEMODEAPPL statement. In z/OS CS V1R4, syntax is obsolete but accepted.	Changed in CS for OS/390 V2R10
VARY TCPIP,,TELNET,ABENDTRAP	Allows you and/or IBM service to get abend dumps based on a return code being set in a given module at the time of failure in Telnet. This command can be used instead of slip traps.	New in z/OS CS V1R2
VARY TCPIP,,TELNET,ACT,luname	Enables <i>luname</i> as a candidate to represent a Telnet client. <i>luname</i> specifies the Telnet logical unit whose status you want to change. This command has no effect on the VTAM state of the LU. In CS for OS/390 V2R10, the <i>luname</i> ALL is used to activate all inactive LUs.	Changed in CS for OS/390 V2R10
VARY TCPIP,,TELNET,DEBUG,	The OFF option is new in z/OS CS V1R2 and in that release it allows you to turn off all debug options on all profiles except for the CONN DROP debug message for connection drops due to errors or timeouts.	New in z/OS CS V1R2

z/OS V1R4 Communications Server release summary

This section describes the Telnet functions new in z/OS V1R4 Communications Server.

Port qualification by linkname or destination IP address

When multiple TCPIP stacks are consolidated, the Telnet port is usually the same on all the original stacks but the stacks have different parameters and mapping statements. In the past, the only consolidation solution was to create new port numbers to retain the different characteristics of the multiple Telnets. The end users had to be notified of the port number change and they were required to make the changes. With port qualification, the end users can all use the same port as long as

the original destination addresses are all moved into the consolidated TCPIP stack. Specifically, z/OS V1R4 allows a single port to have different Telnet characteristics based on the destination IP address or linkname.

Refer to *z/OS Communications Server: IP Configuration Guide* for more information about port qualification.

Restrictions

None.

What this change affects

- Customization

Migration procedures

If you want to take advantage of the port qualification by linkname or destination IP address, perform the tasks in the following table.

Table 141. Port qualification by linkname or destination IP address - Migration tasks

Task	Procedure	Reference
Qualify the port to be used.	If a port qualifier is used, you must specify it on both the TelnetParms and BeginVTAM statements. Specify the nnn,port_qual option on the Telnet Port and SecurePort statements. Specify the nnn,port_qual option on the BeginVTAM Port statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Resolve any errors.	Look for any Telnet debug or other messages to determine the problem.	<i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>

Printer enhancements

In z/OS CS V1R4, printer specification is enhanced in two ways:

- You can specify a default application for printer connections.
- You can specify whether or not the printer session should be dropped when the terminal session is dropped.

Prior to this enhancement, when the terminal emulator partner of an associated printer was dropped, the printer session remained active and the terminal LU was available for the next connection. This could potentially cause a problem for a new user.

Refer to *z/OS Communications Server: IP Configuration Guide* for more information about the Telnet printer enhancements.

Restrictions

None.

What this change affects

- Customization

Migration procedures

If you want to take advantage of the printer enhancements, perform the tasks in the following table.

Table 142. Telnet printer enhancements - Migration tasks

Task	Procedure	Reference
Specify a default application for printer connections.	Code the new BeginVTAM statement PRTDEFAULTAPPL.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Specify whether or not the printer session should be dropped when the terminal session is dropped.	Code DROPASSOCPRINTER. It is allowed in the TelnetGlobals, TelnetParms, and the ParmsGroup statement blocks.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Resolve any errors.	Look for any Telnet debug or other messages to determine the problem.	<i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>

Parameter placement enhancements

In z/OS CS V1R4, parameters are enhanced in the following ways:

- Most parameters are now available in all three information blocks: the TelnetGlobals, TelnetParms, and the ParmsGroup.
- The TelnetDevice statement can now be coded as a parameter in TelnetGlobals, TelnetParms, and the ParmsGroup information blocks. This allows for more granularity when assigning logmodes.
- A PMAP prmgrp_name option is added for the LUMAP and PRTMAP statements to map a ParmsGroup to an LU group. With this addition, parameters can be assigned based on the LU name or group chosen.

Note: A few parameters (LuSessionPend, MSG07, TelnetDevice) can now be coded in both BeginVTAM and as a parameter in the TelnetGlobals, TelnetParms, or ParmsGroup information blocks. Warning messages will be issued when these Telnet parameters are used in BeginVTAM indicating the use is accepted but the preferred placement is in one of the parameter blocks. In a future release, the BeginVTAM placement will not be allowed.

Refer to *z/OS Communications Server: IP Configuration Guide* for more information about the parameter placement enhancements.

Restrictions

None.

What this change affects

- Customization

Migration procedures

None.

New DEBUG option to suppress the connection dropped error messages

In z/OS CS V1R4, a new DEBUG option called EXCEPTION allows the system administrator to turn off all but exception debug messages. This is similar to the OFF option in z/OS CS V1R2. In z/OS CS V1R4, the OFF option is changed to turn off all debug messages. This includes the CONN DROP for error or timeout that are not suppressed by DEBUG EXCEPTION.

DEBUG EXCEPTION is the default in z/OS CS V1R4.

Restrictions

None.

What this change affects

- Customization

Migration procedures

DEBUG EXCEPTION is the default in z/OS CS V1R4. If you coded DEBUG OFF in previous releases and you now want exception messages to be issued, perform the task in the following table.

Table 143. DEBUG EXCEPTION option - Migration task

Task	Procedure	Reference
Turn off all debug messages except the connection dropped error messages.	Code the new EXCEPTION option on the DEBUG statement.	<i>z/OS Communications Server: IP Configuration Reference</i>

New QINIT option for default applications

When an end user logs off an application that is defined as a LOGAPPL application, the normal response of Telnet is to send a USSMSG10 or solicitor screen to the end user. z/OS CS V1R4 introduces a new QINIT option as a mutually exclusive alternative to LOGAPPL on the DEFAULTAPPL, PRTDEFAULTAPPL, LUMAP-DEFAPPL, and PRTMAP-DEFAPPL statements. The QINIT option allows Telnet to reestablish the session when logging off the LOGAPPL application instead of sending a USSMSG10 or solicitor screen. Specifying the QINIT option instead of LOGAPPL therefore allows you to use LOGAPPL function while keeping the original behavior of DEFAULTAPPL or DEFAPPL.

Restrictions

None.

What this change affects

- Customization

Migration procedures

If you want to take advantage of the new QINIT option, perform the task in the following table.

Table 144. Default application QINIT option - Migration task

Task	Procedure	Reference
Use the function provided by LOGAPPL while keeping the original behavior of DEFAULTAPPL or DEFAPPL.	Specify QINIT on the DEFAULTAPPL, PRTDEFAULTAPPL, LUMAP-DEFAPPL, and PRTMAP-DEFAPPL statements. It is a mutually exclusive alternative to LOGAPPL.	<i>z/OS Communications Server: IP Configuration Reference</i>

LU mapping enhancements

z/OS CS V1R4 introduces the following enhancements that are related to LU mapping:

- Telnet can now be instructed to use sequential LU name lookup or select the first LU available in the pool each time. Sequential LU lookup is the default method in z/OS CS V1R4. The z/OS CS V1R2 and earlier default method was to select the first LU available each time.

- Telnet wildcard capability has been expanded beyond numeric or alphabetic range specification. Now each individual character position can be defined as Fixed, Numeric, Alphabetic, Alphanumeric, Hexadecimal, or as a wildcard.
- LU names can be retained (or kept) for a specified period of time after the name has been released. While in the kept state, only the same Client Identifier can reconnect and use the same name again. To all other Client Identifiers the LU name will not be available. Once the specified keep time is reached, any Client Identifier can be assigned the LU.
- Capacity checks can now be specified for LU or PRT groups. When the in-use number reaches the capacity check limit, defined as a percentage of the total, a message will be issued warning that the LU pool is reaching its limit.
- LU naming exits can be written by the system administrator. Instead of defining the LU names in an LU or PRT group, the system administrator can identify the group as an exit and assign the same name as the exit assembler program. The group is defined as an exit in Telnet. When Telnet performs LU lookup, it will call the exit routine that was loaded during profile processing and let the exit generate an LU name.

Restrictions

None.

What this change affects

- Customization

Migration procedures

If you want to take advantage of the LU mapping enhancements, perform the tasks in the following table.

Table 145. LU mapping enhancements - Migration tasks

Task	Procedure	Reference
Specify Sequential LU name lookup method.	Specify the SequentialLU/NoSequentialLU parameter statement. It is available in the TelnetGlobals, TelnetParms, and ParmsGroup statement blocks.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Keep an LU name for a period of time after the name has been released.	Specify the KeepLU parameter statement. It is available in the TelnetGlobals, TelnetParms, and ParmsGroup statement blocks.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Perform a capacity check for LU or PRT groups.	Specify a capacity percentage on LUGROUP and PRTGROUP statements.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Write LU naming exits.	Code LU exit routines to validate or select an LU name used to represent the client. The entry point name must match the routine name specified as the LUGROUP group name. Each LU exit routine specified must be assembled and link-edited as a stand-alone load module.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Upgrade TN3270 SSL to use TLS

In z/OS CS V1R4, TN3270 is upgraded to support the TLS V1 protocol for secure connections.

Restrictions

The TN3270 client must also support TLS.

What this change affects

- Customization

Migration procedures

There are no migration procedures associated with this function. No changes are required. If a TN3270 client requests TLS, a TLS protected session will be started. The display Telnet connection detail report is updated to include the protocol (SSLV2, SSLV3, TLSV1) that is in use for the connection.

z/OS V1R2 Communications Server release summary

This section describes the Telnet functions new in z/OS V1R2 Communications Server.

z/OS UNIX Telnet (otelnetd) server – Kerberos support

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications using secret-key cryptography. The Kerberos support provided in z/OS V1R2 Communications Server provides greater security for certain applications and allows the use of these applications to secure data traffic in the network. Specifically, z/OS V1R2 Communications Server introduces Kerberos support for authentication for the following applications:

- The UNIX remote shell execution (rsh) server — authentication support provided by the Kerberos 5 protocol and the GSSAPI protocol
- The FTP client and FTP server — authentication support provided by the GSSAPI protocol
- The UNIX Telnet server — authentication support provided by the Kerberos 5 protocol

If you are using UNIX Telnet, FTP, or UNIX RSHD, you must add these Kerberos data sets:

- EUVF.SEUVFLNK - add to the LNKLSTxx PARMLIB member
- EUVF.SEUVFLPA - add to the LPALSTxx PARMLIB member

The Kerberos support for the UNIX Telnet server is described in this section. See “z/OS UNIX RSHD Kerberos support” on page 111 for the UNIX RSHD server considerations. See “Kerberos support for the FTP server and client” on page 185 for the FTP client and FTP server considerations.

Restrictions

None.

Incompatibilities

The zSeries KDC is incompatible with Windows 2000 Kerberos applications. Windows 2000 applications must use the Windows KDC. To support Windows 2000 applications, a cross-realm connection between the zSeries KDC and the Windows KDC is required.

What this change affects

- Security
- Customization
- Operations

Migration procedures

If you want to take advantage of the Kerberos support function for the UNIX Telnet server, perform the task in the following table. See “z/OS UNIX RSHD Kerberos support” on page 111 for the UNIX RSHD server considerations. See “Kerberos support for the FTP server and client” on page 185 for the FTP client and FTP server considerations.

Table 146. Kerberos support for the UNIX Telnet server - Migration tasks

Task	Procedure	Reference
Specify authentication mode in the otelnetd server.	Specify the -a parameter when invoking the otelnetd server.	<i>z/OS Communications Server: IP Configuration Reference</i>
Disable use of Kerberos Version 5 authentication in the otelnetd server.	Specify the -X parameter when invoking the otelnetd server.	<i>z/OS Communications Server: IP Configuration Reference</i>

TN3270 diagnostics enhancements

The DEBUG function was introduced in CS for OS/390 V2R10 (see “TN3270 DEBUG” on page 228) to aid in tracking major state changes and to provide connection ID and LU name information. In z/OS V1R2 Communications Server, DEBUG diagnostics are enhanced in the following ways:

- A new Telnet DEBUG option, Trace, has been added to display data to and from the client and to and from VTAM. The VTAM data will include the RPL. To prevent message flooding, Telnet will issue these messages for only one client. Once the option is turned on by Obeyfile, the next connection that maps to the DEBUG TRACE parameter will use message EZZ6035I to display data passing through Telnet. ParamsGroup can be used to very accurately select the client in question.
- A VARY DEBUG command was added to turn off all DEBUG options on all profiles. When the VARY DEBUG OFF command is issued, all DEBUG messages are suppressed for connections associated with all profiles, including the current profile. To turn on DEBUG again, issue the Obeyfile with the DEBUG option specified.
- You can set an abend trap. You can set the trap by specifying a module name (or wildcard module name) and optionally specifying a return code and instance number. The abend trap feature allows you to set up for a dump of the TCP address space at the time of failure in Telnet. This is an improvement over previous releases when IBM service was required to send you an updated module containing an abend trap.
- The new SMF format 119 records are now available; see “SMF recording enhancements” on page 121 for details.

Restrictions

None.

What this change affects

- Customization
- Diagnosis

Migration procedures

If you want to take advantage of the TN3270 diagnostics enhancements, perform the tasks in the following table.

Table 147. TN3270 diagnostics enhancements - Migration tasks

Task	Procedure	Reference
Enable DEBUG trace.	Specify the DEBUG TRACE parameter.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Diagnose the trace data.	Interpret the traced data if capable. Otherwise, call IBM service for assistance.	Various RFCs describe Telnet protocol.
Disable all DEBUG activity.	Specify the operator command VARY TCPIP,,TELNET,DEBUG,OFF	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP System Administrator's Commands</i>
Obtain an abend dump based on the return code that is set in a given module at the time of failure.	Specify the operator command VARY TCPIP,,TELNET,ABENDTRAP, <i>module,rcode,instance</i>	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP System Administrator's Commands</i>

TN3270E RFC 2355 SNA extensions

Through the SNA extensions implementation, IBM allows TN3270E clients to connect to the TN3270E Server using the Contention Resolution function and SNA Sense function as documented in the Internet Draft for TN3270E Functional Extensions of RFC 2355. The TN3270E Functional Extensions enhance the SNA-like capability of the TN3270E connections. Both the Contention Resolution and SNA Sense functions are negotiated between the TN3270E Client and the TN3270E Server when the connection is established, and those functions will be used during the connection *if* both the client and server agree.

Restrictions

Both the TN3270E client and server must support the TN3270E Functional Extensions. SNAExt must be coded or allowed to default to SNAExt in the TN3270E Server profile.

What this change affects

- Usability

Migration procedures

No action is required to take advantage of the SNA extensions; it is the default. If you do *not* want to take advantage of the SNA extensions, perform the second task in the following table.

Table 148. TN3270E RFC 2355 SNA extensions - Migration tasks

Task	Procedure	Reference
Enable SNA extensions.	No action is required; support of the SNA extensions is the default. Optionally, specify the SNAExt parameter.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Disable SNA extensions.	Specify the NoSNAExt parameter.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

TN3270 profile and display enhancements

The following enhancements are made to the Telnet profile in z/OS V1R2 Communications Server:

- The scope of how Telnet parameters apply to connections is enhanced by making several parameters available in TelnetGlobals, TelnetParms, and ParmsGroup. This allows greater control over the granularity of these parameters.
- Additional Client Identifiers are defined for mapping purposes.
- Display output for profile mapping statements is standardized based on the Mapping Objects to Client Identifiers concept.

These enhancements are discussed in the following sections.

Telnet parameters enhancements

The following Telnet parameters can now be specified in TelnetGlobals, TelnetParms, or ParmsGroup:

- LUSESSIONPEND/NOLUSESSIONPEND
- MSG07/NOMSG07
- TN3270E/NOTN3270E
- SNAEXT/NOSNAEXT
- SIMCLIENTLU/NOSIMCLIENTLU
- FULLDATATRACE/NOFULLDATATRACE
- EXPRESSLOGON/NOEXPRESSLOGON
- INACTIVE
- KEEPINACTIVE
- PRTINACTIVE
- SCANINTERVAL
- TIMEMARK
- SSLTIMEOUT
- SMFINIT/SMFTERM
- CODEPAGE

Some of the parameters have a NO option. This gives you complete control of the function at any level to turn it on or off. In addition, more than one ParmsGroup Object may now be mapped to a single Client Identifier. The parameters are applied to the client connection in the order they are mapped. For example, an early mapping of PRMGRP1 that contains DEBUG DETAIL will be overridden by a later mapping of PRMGRP2 that contains DEBUG SUMMARY. The end result for the client connection will be DEBUG SUMMARY.

Note: Prior to z/OS CS V1R2, specifying 0 for TIMEMARK or SCANINTERVAL would result in the default value. This was not consistent with other timers (for other timers, specifying 0 would result in turning off the timer). Therefore, in z/OS CS V1R2 and later, it is not possible to specify 0 for TIMEMARK or SCANINTERVAL. If you coded 0 in previous releases for the SCANINTERVAL or TIMEMARK value, you must change this to a valid value. The valid range for TIMEMARK and SCANINTERVAL is from 1-9999.

Additional Telnet Client Identifiers

Clients map to Telnet Objects, such as LUs, application names, and USS tables, by using their Client Identifiers. Prior to this release, Client Identifiers included the following:

- The client's exact IP address or the IP address group
- The client's exact hostname or hostname group
- The client's host linkname

This release introduces additional Client Identifiers to provide more ways to map Objects to clients. New Client Identifiers include user IDs, destination IP addresses, and groupings of these. In addition, a linkname group has been created.

Specifically, Telnet Client Identifiers are enhanced in the following ways:

- A user ID can be derived from the Client Certificate allowing mapping statements using an eight character name rather than certificates. The certificate is saved after SSL negotiation and a RACROUTE call is made to derive the user ID.
- You can now specify destination IP addresses when using dynamic Virtual IP Addresses (VIPAs). A destination IP address is a host address that is the destination for a Telnet connection. A linkname can be used as a Client Identifier to map Objects to destination IP addresses when the linkname is static and defined in the profile. However, if the destination IP address is a dynamic VIPA, the linkname is not known before a new VIPA is created. In this case, destination IP address is the ideal solution. In other cases, specifying the destination IP address in the Telnet profile may be more clear than specifying the linkname.
- Groups of each Client Identifiers are also valid. Like IP and hostname, user IDs and wildcard user IDs can be grouped into USERGROUPS. Destination IPs and subnet masks can be grouped into DESTIPGROUPS. Linkname and wildcard linknames can be grouped into LINKGROUPS.

USERIDs and LINKNAMEs can be wildcard names when in a group statement. Destination IP addresses can be subnet masks when in a group statement.

Enhanced display output

Telnet mapping displays have been standardized and more detail is provided on the Profile detail and Connection detail displays. Specifically, mapping displays are enhanced as follows.

- All mapping statements in Telnet conform to the mapping rule:

```
MAP OBJECTS TO CLIENTS BASED ON CLIENT IDENTIFIER
```

Consequently, it makes sense to standardize Profile mapping statement displays to uniformly provide mapping information for all Objects and Client Identifiers. Two new displays have been added: an OBJECT display and a CLIENTID display. Both displays present the same mapping information but the information is sorted based on either Object or Client Identifier. The information presented is at least as detailed as the existing profile mapping displays. The old displays are no longer needed but their display commands continue to be supported with their output conforming to the new display output.

- The Profile detail display has been changed to show ALL parameter values and what the source of the value is. It may be a default value, a TelnetGlobals value, or a TelnetParms value. The Connection detail display presents the mapping information in a more readable format and shows all parameters in summary form for that connection.

Restrictions

The USERID Client Identifier is derived from the Client Certificate by an SAF product such as RACF. The connection must be SSL with the ClientAuth SAFCERT option in effect.

What this change affects

- Customization
- Usability

Migration procedures

If you want to take advantage of the additional granularity of Telnet parameters or the new Client Identifiers, you must customize the Telnet profile. Perform the tasks in the following table.

Table 149. TN3270 profile and display enhancements - Migration tasks

Task	Procedure	Reference
Understand the implications of parameter placement.	Read the appropriate section of the Telnet chapter in <i>z/OS Communications Server: IP Configuration Guide</i> .	<i>z/OS Communications Server: IP Configuration Guide</i>
Understand the concept of the new Client Identifiers.	Read the mapping section of the Telnet chapter.	<i>z/OS Communications Server: IP Configuration Guide</i>
Define a client identifier.	Specify the type or ID of the client identifier you want to use. Label your client identifiers' type on the mapping statement to avoid confusion. This is optional except when you are using an exact USERID or a destination IP address. When you are using an exact USERID or a destination IP address, you must identify the type; otherwise, it will be assumed to be a linkname of Client IP Address.	<i>z/OS Communications Server: IP Configuration Reference</i>
Map Telnet objects, such as LU, using a client identifier.	Specify the object you want to map. For example, specify the USERID name on the LUMAP statement to map a certain LUGROUP to the USERID.	<i>z/OS Communications Server: IP Configuration Reference</i>

Express Logon Feature using TN3270E Server on z/OS

The Express Logon Feature was introduced in CS for OS/390 V2R10 for both three-tier and two-tier Telnet configurations; see “Express Logon feature: Digital Certificate Access Server (DCAS)” on page 155. The three-tier solution uses an outboard Telnet server and requires the use of the Digital Certificate Access Server (DCAS). The two-tier solution, introduced by APAR PQ47742 in CS for OS/390 V2R10, is part of the base TN3270 Telnet Server in z/OS V1R2. The two-tier solution does not require DCAS because this function is performed by the TN3270 Telnet Server. Refer to *z/OS Communications Server: IP Configuration Guide* for a discussion of the two-tier versus the three-tier approach.

This feature requires the client to provide an X509 V3 certificate for translation to a userid. The client also has to provide an application name using the New_Environment protocol. Once the certificate and the application names are received by the TN3270/E server, the server will supply the userid and password to the VTAM application.

This feature is activated in the server by way of the ExpressLogon parameter in the Telnet profile.

Restrictions

Your connection must be through SSL and it must have client authentication through SAF (CLIENTAUTH SAFCERT) or you cannot use this function. The client must support macro scripts and RFC 1572, the New_Environment protocol. Host On Demand Version 5 meets these requirements. Refer to *z/OS Security Server RACF Security Administrator's Guide* for information on client authentication.

What this change affects

- Usability

Migration procedures

If you want to take advantage of the Express Logon Feature using TN3270E Server on z/OS function, perform the tasks in the following table.

Table 150. Express Logon Feature using TN3270E server on z/OS function - Migration tasks

Task	Procedure	Reference
Enable Express Logon.	Specify EXPRESSLOGON parameter.	<i>z/OS Communications Server: IP Configuration Guide and z/OS Communications Server: IP Configuration Reference</i>
Interpret Express Logon fields on the Display PROFILE and Display CONNECTION commands.	Specify D TCPIP,,T,PROF or D TCPIP,,T,CO,CO=xx.	<i>z/OS Communications Server: IP User's Guide and Commands and z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>

Communications Server for OS/390 V2R10 release summary

This section describes the Telnet functions new in CS for OS/390 V2R10.

The UNIX Telnet server (otelnetsd) enhancements

The otelnetsd command is enhanced as follows:

- When a new otelnetsd command-line option, -D login, is specified, otelnetsd will write a concise summary of login and logout activity to the syslog facility "auth".
- When a new otelnetsd command-line option, -T terminfo-directory, is specified, otelnetsd will set the TERMINFO environment variable to the specified value prior to searching for the terminfo definition for the terminal type specified by the Telnet client. This facility should be used if the administration has configured installation-defined terminfo definitions.

Restrictions

None.

What this change affects

- Customization
- Security
- Usability

Migration procedures

If you want to take advantage of the otelnetsd enhancements, perform the tasks in the following table.

Table 151. otelnetsd enhancements - Migration tasks

Task	Procedure	Reference
Enable login/logout trace.	Specify -D login on the otelnetsd command line in the inetd configuration file (for example, /etc/inetd.conf).	<i>z/OS Communications Server: IP Configuration Reference and IP Messages</i>
Enable otelnetsd to find terminfo definitions in installation-defined directories.	Specify -T terminfo-directory on the otelnetsd command line in the inetd configuration file.	<i>z/OS Communications Server: IP Configuration Reference and z/OS UNIX System Services Planning</i>

TN3270 SSL enhancement

This function is an enhancement to Secure Sockets Layer (SSL), which was introduced in CS for OS/390 V2R6. Previously, SSL connections and basic connections had to be supported by separate ports. With this enhancement, the server can use the SECUREPORT statement to allow a single port to support both secure and basic connections. Based on the client's IP address, host name, or linkname, the server can specify whether or not a connection will use SSL protocols.

To provide this control, a PARMSGROUP block is added to the BEGINVTAM block and is used to specify the connection type (CONNTYPE) associated with a subset of the port's connections. The PARMSMAP statement is used to associate the PARMSGROUP information with particular IP addresses, host names or linknames. If no changes are made to the existing profiles, SECUREPORT will only allow connections that are protected with the SSL protocol.

The TN3270 SSL enhancement also supports the Internet Engineering Task Force (ietf) TLS-based Telnet Security draft which allows the client and server to negotiate whether or not the connection will be protected with SSL protocols. Refer to *z/OS Communications Server: IP Configuration Guide* for details.

If a CONNTYPE SECURE is specified (which is the default CONNTYPE for a SECUREPORT) and the standard SSL fails due to a handshake time out, Telnet will automatically try to connect using the Internet Engineering Task Force (ietf) TLS-based Telnet Security draft's negotiated SSL protocol. If the client does not agree to negotiate SSL, then the connection is closed. This support is provided for installations that do not know what type of SSL is in use by each client. CONNTYPE NEGTSURE is provided for cases where the client is known to support only the negotiated SSL protocol.

Restrictions

To use CONNTYPE NEGTSURE, the client must also support the Internet Engineering Task Force (ietf) TLS-based Telnet Security draft.

What this change affects

- Customization
- Operations

Migration procedures

The TN3270 Negotiated SSL function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 152. TN3270 Negotiated SSL - Migration tasks

Task	Procedure	Reference
Allow a single port to support both secure and basic connections and specify SSL or debug options based on connection IP address, linkname, or host name.	Use the SECUREPORT statement and specify PARMSGROUP and PARMSMAP information in the BEGINVTAM block.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Negotiate an SSL connection using the Internet Engineering Task Force (ietf) TLS-based Telnet Security draft SSL protocol.	Specify CONNTYPE NEGTSURE with the SECUREPORT statement in the TELNET PROFILE.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

Table 152. TN3270 Negotiated SSL - Migration tasks (continued)

Task	Procedure	Reference
Control connection type used by client.	Specify new PARMSGROUP, PARMSMAP and CONNTYPE statements in the TELNET PROFILE.	<i>z/OS Communications Server: IP Configuration Reference</i> and <i>z/OS Communications Server: IP Configuration Guide</i>

TN3270 System SSL

Like TN3270 Negotiated SSL, this function is an enhancement to SSL, which was introduced in CS for OS/390 V2R6. This enhancement upgrades SSL support to use OS/390's Cryptographic Services System Secure Sockets Layer (System SSL).

System SSL contains performance improvements that allow for more linear scalability in multiprocessor environments. The OS/390 Security Server supports the use of RACF as a repository for the server's key ring. This support is referred to as Common Key Ring Support. The TN3270 server now supports RACF's Common Key Ring support as an optional alternative to using the HFS or MVS data set to store the key ring.

In addition, Certificate Revocation List (CRL) processing for client certificates issued by Vault Registry is now supported. (Vault Registry is an IBM product that provides the software necessary for an entity to become a Certificate Authority.) System SSL supports an optional query to an LDAP directory to determine if the client-supplied certificate is in the CRL that is maintained on the LDAP directory. System SSL can provide this support if the client certificate was created by Vault Registry.

Restrictions

The TN3270 server requires access to the Cryptographic Services System SSL data link libraries (DLLs) located in the *hlq.SGSKLOAD* partitioned data set. If using Telnet SSL support, this library must be:

- In the linklist or included in the TCP started procedure STEPLIB or JOBLIB DD
- APF-authorized

Incompatibilities

The encryption services DLLs used by the TN3270 server are no longer shipped with the OS/390 IBM Communications Server. Instead, the OS/390 Cryptographic Services System SSL DLLs are used. Therefore, the level of encryption available to the TN3270 server is based on the installed level of the OS/390 Cryptographic Services: System SSL.

Some earlier versions of SSL determined the encryption type used for a connection based on the client's preference. System SSL uses the server's preferences when selecting the encryption type for the connection. If you code an ENCRYPT block in the TELNETPARMS, ensure that the encryption types are listed in order of preference. The display profile detail is changed to list the encryption type in the order specified.

What this change affects

- Customization
- Operations
- Installation

Migration procedures

Any installation currently using Telnet's SSL support *requires* completing the *first three tasks* in the following table. The remaining tasks are optional.

Table 153. TN3270 System SSL - Migration tasks

Task	Procedure	Reference
Required; ensure the required level of OS/390 Cryptographic Services: System SSL is installed.	If your installation requires triple DES or 128-bit encryption, then the level 3 feature of OS/390 Cryptographic Services: System SSL is required. All other levels of encryption are available with the base product.	<i>z/OS Program Directory</i>
Required; set up access to the Cryptographic Services Security's DLLs.	This is located in <i>hlq.SGSKLOAD</i> by default. If using Telnet SSL support, this library must be: <ul style="list-style-type: none"> In the linklist or included in the TCP started procedure STEPLIB or JOBLIB DD APF-authorized 	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS System Secure Sockets Layer Programming</i>
Required; set up access to the C Run-Time Library (SCEERUN) and the C/C++ IBM Open Class® Library (SCLBDLL)	These libraries must be: <ul style="list-style-type: none"> In the linklist or included in the TCP started procedure STEPLIB or JOBLIB DD APF-authorized 	<i>z/OS Communications Server: IP Configuration Guide</i>
Optional; use RACF as a repository for the server's key ring.	Specify a RACF-based keyring. The RACF userid associated with the stack must have update control to the <i>irr.digcert.listring</i> in the FACILITY class: <ul style="list-style-type: none"> Ensure that the DIGTCERT and DIGTRING classes are active before defining certificates or keyrings to RACF. Build your RACF key ring. Update the TELNETPARMS KEYRING statement (KEYRING SAF keyringname) 	<i>z/OS Security Server RACF Security Administrator's Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Optional; check client certificates issued by Vault Registry against the Vault Registry Certificate Revocation List.	<ul style="list-style-type: none"> Add a TELNETGLOBALS block and specify the CRLLDAPSERVER information. Set up access to the LDAP Server Library (<i>hlq.SGLDLNK</i>). This library must be in the linklist or in the TCP started procedure's STEPLIB or JOBLIB DD and must be APF-authorized. Specify CLIENTAUTH in the TELNETPARMS or PARMSGROUP. 	<i>z/OS Communications Server: IP Configuration Reference</i>
Optional; limit encryption types.	Code the encryption types in order of preference in the ENCRYPT/ENDENCRYPT block.	<i>z/OS Communications Server: IP Configuration Reference</i>

TN3270 enhanced SLU simulation

This function enhances Telnet's simulation of SNA Secondary LUs (SLUs). Previously, when the SLU requested a session with an unavailable Primary LU (PLU), the session request was rejected and the SLU was inactivated. Depending on Telnet profile setup, the end user either received a USSMSG07 error or the connection was dropped. This OS/390's Cryptographic Services System Secure Sockets Layer (System SSL) enhancement allows SLU simulation to avoid these situations by including the following functions:

- **KEEPOPEN function:** The KEEPOPEN parameter allows Telnet to keep the SLU LU ACB open instead of closing it after a failed session attempt.
- **LOGAPPL function:** The LOGAPPL function allows clients to request a session with a PLU and then wait for the PLU if it is currently inactive. When the PLU becomes active, it will initiate a session with the waiting client.

Restrictions

None.

What this change affects

- Customization
- Availability

Migration procedures

The TN3270 enhanced SLU simulation function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 154. TN3270 enhanced SLU simulation - Migration tasks

Task	Procedure	Reference
Enable the Telnet secondary LU ACB to remain OPEN so it can accept a session request initiated by the host application.	Specify KEEPOPEN on the LUMAP statement.	<i>z/OS Communications Server: IP Configuration Reference</i>
Allow clients to request a session with PLU and wait for the PLU to become active if it is currently inactive.	Specify LOGAPPL applname on the LUMAP, DEFAULTAPPL, or LINEMODEAPPL statement.	<i>z/OS Communications Server: IP Configuration Reference</i>

TN3270 NQN enhancement for the TN3270E server

This enhancement expands the Network Qualified Name (NQN) support included in CS for OS/390 V2R8 to include the DEFAULTAPPL and LINEMODEAPPL profile statement, a network-qualified logon from the solicitor panel, and a network-qualified logon in linemode.

Restrictions

None.

What this change affects

- Customization

Migration procedures

If the end-user is specifying a network-qualified name (NQN), the TN3270 NQN enhancement for the TN3270E server function is automatically enabled. If the default NQN applications are desired, perform the task in the following table.

Table 155. TN3270 NQN enhancement for the TN3270E server - Migration tasks

Task	Procedure	Reference
Enable NQN support in the TN3270 profile.	Specify the NQN formatted application name on DEFAULTAPPL and LINEMODEAPPL statements in the TN3270 profile.	<i>z/OS Communications Server: IP Configuration Reference</i>

TN3270 client reconnect to TN3270E server

This function is an enhancement to the TN3270 - Takeover function that was introduced in CS for OS/390 V2R8. With the CS for OS/390 V2R8 TN3270 -

Takeover, the old session and old connection were dropped, allowing for the re-creation of the session from the beginning. This enhancement maintains the SNA session and allows the reconnection to be less disruptive. This is accomplished by a new keyword, TKOSPECLURECON (which is mutually exclusive with the current TKOSPECLU), in TELNETPARMS statements.

Restrictions

None.

What this change affects

- Customization
- Availability

Migration procedures

The TN3270 client reconnect to TN3270E server does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 156. TN3270 client reconnect to TN3270E server - Migration task

Task	Procedure	Reference
Recover from loss of connectivity.	Specify TKOSPECLURECON nnnnnnnn on TELNETPARMS, where nnnnnnnn is the number of seconds the server waits before checking to see if a response was received from the original client.	<i>z/OS Communications Server: IP Configuration Reference</i>

TN3270E resource pooling

Prior to this release, an SNA LU name was either:

- Assigned by the server (this was the default, called *generic*)
- Specified by the client (called *specific*).

This enhancement allows TN3270E clients to specify an LU pool when choosing an SNA LU name. Included in this enhancement are several functions. The client can now:

- Specify a default LU group for specific LU requests.
- Specify a default printer group for generic printer requests.
- Specify a default printer group for specific printer requests.
- Specify an LUGROUP name on a TN3270E specific request.
- Specify LU group names on ALLOWAPPL and RESTRICTAPPL statements.
- Use a new option to specify that generic TN3270E requests should wait until the application is known before choosing an LU. Lookup is done as if the connection were TN3270, but all TN3270E functions remain.
- Code multiple LUMAP or PRTMAP statements for the same IPGROUP. This is especially useful when used with LOGAPPL and specific request clients.

Restrictions

None.

What this change affects

- Customization
- Availability
- Usability

Migration procedures

The TN3270E resource pooling does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 157. TN3270E resource pooling - Migration tasks

Task	Procedure	Reference
Define and display default specific LU group.	Add DEFAULTLUSSPEC luname and ENDDEFAULTLUSSPEC to your TN3270 profile.	<i>z/OS Communications Server: IP Configuration Reference</i>
Define and display default printer group.	Add DEFAULTPRT prtname and ENDDEFAULTPRT to your TN3270 profile	<i>z/OS Communications Server: IP Configuration Reference</i>
Define and display default specific printer group.	Add DEFAULTPRTSPEC prtname and ENDDEFAULTPRTSPEC to your TN3270 profile.	<i>z/OS Communications Server: IP Configuration Reference</i>
Specify LU group names on ALLOWAPPL and RESTRICTAPPL statements.	Specify the new option LUG lugroup name on ALLOWAPPL and RESTRICTAPPL statements.	<i>z/OS Communications Server: IP Configuration Reference</i>
Use the new option for simulated TN3270 LU selection for TN3270E clients operating with generic selection of terminal LUs.	Specify SIMCLIENTLU on TELNETPARMS.	<i>z/OS Communications Server: IP Configuration Reference</i>

TN3270 DEBUG

CS for OS/390 V2R10 introduces a new DEBUG function to aid in tracking major state changes and to provide connection ID and LU name information. The DEBUG function has two parameters; SUMMARY lists the state changes of the connection, and DETAIL issues a message with connection information at the time of failure. Refer to *z/OS Communications Server: IP Configuration Guide* for more information on DEBUG SUMMARY and DEBUG DETAIL.

Restrictions

None.

What this change affects

- Diagnosis

Migration procedures

The TN3270 DEBUG function does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 158. TN3270 DEBUG function - Migration task

Task	Procedure	Reference
Track major state changes and/or view connection ID and LU name information.	Code the DEBUG statement in the TELNETPARMS block.	<i>z/OS Communications Server: IP Configuration Guide</i>

TN3270 Timemark default change

The default Scaninterval/Timemark values are increased from 120/600 seconds to 1800/10800 seconds. The new values are the IBM recommended values to avoid network flooding of Timemarks during periods of low activity.

Restrictions

None.

What this change affects

- Customization

Migration procedures

The TN3270 Timemark default change does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 159. TN3270 Timemark default change function - Migration task

Task	Procedure	Reference
If you were using the old default values and still want those values, Scaninterval/Timemark must now be coded.	Code the SCANINTERVAL and/or TIMEMARK statement in the TELNETPARMS block.	<i>z/OS Communications Server: IP Configuration Guide</i>

Chapter 11. Migrating the SNMP server and client

Simple Network Management Protocol (SNMP) is a network management protocol that is used to monitor network elements attached to the TCP/IP internet.

This chapter contains an overview of SNMP and its various components; see “SNMP overview”.

This chapter also contains new and changed SNMP interfaces, including:

- “SNMP configuration files” on page 234
- “SNMP operator commands” on page 234
- “SNMP z/OS UNIX commands” on page 235
- “SNMP environment variables” on page 235
- “SNMP agent MIB modules” on page 235
- “TCP/IP subagent MIB modules” on page 236
- “Service Level Agreement subagent MIB modules” on page 236

This chapter also contains the following for SNMP:

- “z/OS V1R4 Communications Server release summary” on page 236
- “z/OS V1R2 Communications Server release summary” on page 237
- “Communications Server for OS/390 V2R10 release summary” on page 240

In this chapter, file names appear in uppercase to indicate that files can reside in different locations. For information about search orders, refer to the *z/OS Communications Server: IP Configuration Reference*.

SNMP overview

SNMP defines an architecture that consists of:

- Network management applications
- Network management agents and subagents
- Network elements, such as hosts and gateways

The SNMP network management application can ask agents for specific information about network elements. Conversely, agents can tell the network management application when something happens to one or more network elements. The protocol used between the network management application and agents is SNMP. The transport protocol for SNMP requests is the User Datagram Protocol (UDP).

SNMP defines both the network management data and the ways in which the data is retrieved or changed by the network management application. Examples of network management data include device definitions, counts of packets received at the IP layer, TCP connection data, and so forth. The information about the network elements is stored in the Management Information Base (MIB), which is supported by the SNMP agent and its subagents. A MIB variable (or MIB object) is a specific instance of data in a collection of objects related to a common management area. The collection is called a *MIB module*.

The z/OS CS Network Management agent and subagents, also called SNMP agent and SNMP subagents, support many standard (RFC-based) MIB modules. The SNMP TCP/IP subagent also supports enterprise-specific MIB modules. For information on MIB modules supported by the z/OS CS SNMP agent and

subagents, see the SNMP agent capabilities statement, shipped as HFS file /usr/lpp/tcpip/samples/mvstcpip.caps. Additionally, enterprise-specific MIBs are documented in the /usr/lpp/tcpip/samples HFS directory. See “TCP/IP subagent” for more information on enterprise-specific MIB modules supported by the TCP/IP subagent. For a complete list of MIB objects supported by the SNMP agent and subagents shipped with z/OS CS, refer to *z/OS Communications Server: IP System Administrator's Commands*.

Network management application

The stations that monitor network elements run *network management applications*. In z/OS CS, the `osnmp` command provides SNMP network management from the z/OS UNIX shell. The NetView SNMP command provides network management from the NetView command line. Like the SNMP command in the NetView environment, the `osnmp` command is used to retrieve or change data from SNMP and monitor for asynchronous events known as *notifications*. An unconfirmed notification is called a *trap*. A confirmed notification is called an *inform*.

For information about the syntax and use of the `osnmp` and NetView SNMP commands, refer to *z/OS Communications Server: IP User's Guide and Commands* and *z/OS Communications Server: IP System Administrator's Commands*.

SNMP agent

In z/OS CS, the SNMP agent is a z/OS UNIX application. It supports SNMPv1, SNMPv2c, and SNMPv3. SNMPv2c offers protocol enhancements such as the GETBULK operation. SNMPv3 provides a network management framework that allows the use of user-based security in addition to, or instead of, the community-based security supported in SNMPv1 and SNMPv2c. The view-based access control model supported in SNMPv3 allows granular access control for MIB objects with either the user-based or community-based security models. SNMPv3 also enables dynamic changes to the SNMP agent configuration.

For details on setting up the SNMP agent, refer to *z/OS Communications Server: IP Configuration Guide*. For details on the syntax of configuration files and search orders, refer to *z/OS Communications Server: IP Configuration Reference*.

SNMP subagents

A subagent extends the set of MIB variables supported by an SNMP agent. z/OS CS supports three subagents: a TCP/IP subagent, an OMPROUTE subagent, and a Service Level Agreement (SLA) subagent. For a complete list of MIB objects, refer to *z/OS Communications Server: IP System Administrator's Commands*.

TCP/IP subagent

The TCP/IP subagent in z/OS CS is a z/OS UNIX application that runs in its own task in the TCP/IP address space. This subagent supports many standard (RFC-based) MIB objects. In addition, it supports MIB objects in the following enterprise specific MIB modules:

- The IBM 3172 enterprise specific MIB.
- The IBM MVS TCP/IP enterprise-specific MIB. This MIB defines objects to extend standard MIB tables, supports retrieval and change of TCP/IP address space configuration parameters, and provides management support for the environments where Asynchronous Transfer Mode (ATM) is used.

The TCP/IP subagent support evolves with each release. New MIB objects may be supported, and, occasionally, old ones may be removed for functions that are no

longer relevant. This is particularly true for the MIB objects in the IBM MVS TCP/IP enterprise-specific MIB. This MIB's definition is shipped as HFS file /usr/lpp/tcpip/samples/mvstcpip.mi2. All changes to this MIB are listed both in the release-specific sections of this chapter and in the REVISION sections of the shipped MIB definition.

The TCP/IP subagent in z/OS CS provides SET support, enabling remote configuration of some TCP/IP address space parameters. The TCP/IP subagent is configured and controlled by the SACONFIG statement in the PROFILE.TCPIP data set. Systems where SNMP support is not required can disable the subagent and save system resources.

OMPROUTE subagent

The OMPROUTE subagent implements the Open Shortest Path First (OSPF) MIB variable containing OSPF protocol and state information.

The OMPROUTE subagent supports selected MIB objects defined in Request for Comment (RFC) 1850.

For a detailed description of the OMPROUTE subagent, refer to the *z/OS Communications Server: IP Configuration Reference*.

Service Level Agreement (SLA) subagent

The Service Level Agreement (SLA) subagent allows network administrators to retrieve data and determine if the current set of SLA policy definitions are performing as needed or if adjustments need to be made.

Key generation commands

The pwtokey and pwchange commands are provided to enable generation and change of keys used for authentication and encryption with SNMPv3.

For more information about pwtokey, refer to *z/OS Communications Server: IP Configuration Reference*. For information about pwchange, refer to *z/OS Communications Server: IP System Administrator's Commands*.

Distributed Protocol Interface

The DPI is an application interface used by the SNMP agent to communicate with subagents. With DPI, you can dynamically add, delete or replace management variables supported by the SNMP agent and its subagents. z/OS CS provides DPI V2.0 for z/OS UNIX C socket users and DPI V1.1 for traditional C socket users. DPI V2.0 provides additional function, making it easier to write subagents and simplifying the task of developing and administering your application.

For more information about the DPI, refer to the *z/OS Communications Server: IP Programmer's Reference*.

Trap forwarder daemon

The trap forwarder daemon was new in CS for OS/390 V2R10 and it forwards traps from the SNMP agent to network management applications. It listens for traps on a port, typically 162, and forwards them to all configured managers.

For more information about the trap forwarder daemon, refer to *z/OS Communications Server: IP Configuration Reference*.

New and changed interfaces for SNMP

SNMP configuration files

Table 160. New or changed configuration files (SNMP)

File	Statement or parm	Description	Status
MIBS.DATA		File used to extend the osnmp command's ability to translate MIB object textual name to object identifiers. In VR10, it can be specified using an environment variable, MIBS_DATA.	Changed in CS for OS/390 V2R10
OSNMP.CONF		osnmp command configuration file	
	NOSVIPA	Prevents the osnmp command from using a source VIPA address as the originating address on packets it sends	New in V2R10
SNMPD.CONF	<ul style="list-style-type: none"> NOTIFY_FILTER NOTIFY_FILTER_PROFILE 	Allow the configuration of notification filtering	Changed in CS for OS/390 V2R10
	<ul style="list-style-type: none"> NOTIFY TARGET_ADDRESS 	Changed to allow generation of inform-type notifications	Changed in CS for OS/390 V2R10
	<ul style="list-style-type: none"> SNMP_COMMUNITY TARGET_ADDRESS 	<p>SNMP_COMMUNITY is new in V1R2 and it defines a community for community-based security. Communities defined with this statement may be dynamically changed by using the SNMP SET commands for the snmpCommunityTable. IBM recommends that you use it instead of the COMMUNITY statement.</p> <p>TARGET_ADDRESS defines a management application's address and identifies parameters to be used in sending notifications. It is enhanced in z/OS CS V1R2 to augment the Target_Address table.</p>	SNMP_COMMUNITY is new in z/OS CS V1R2. TARGET_ADDRESS is changed in z/OS CS V1R2.
	May be specified using an environment variable, SNMPTRAP_DEST	New in CS for OS/390 V2R10	
TRAPFWD.CONF		Trap destination configuration file for trap forwarder daemon	New in CS for OS/390 V2R10

SNMP operator commands

Table 161. New or changed operator commands (SNMP)

Command	Description	Status
MODIFY TRAPFWD_procname	Command to direct the trap forwarder daemon to reread its configuration file or to query or set the level of tracing	New in CS for OS/390 V2R10

SNMP z/OS UNIX commands

Table 162. New or changed UNIX commands (SNMP)

Command	Parameter	Description	Status
osnmp	-a	Prevents the osnmp command from using a source VIPA address as the originating address on packets it sends.	New in CS for OS/390 V2R10
osnmpd	-a	Prevents the SNMP agent from using a source VIPA address as the originating address on packets it sends for responses, traps, and informs.	New in CS for OS/390 V2R10
trapfwd		Command to start the trap forwarder daemon. The trap forwarder daemon can be used to allow multiple network managers to monitor for traps at the same IP address.	New in CS for OS/390 V2R10

SNMP environment variables

Table 163. New or changed environment variables (SNMP)

Environment variable	Application	Description	Status
MIBS_DATA	osnmp command	Specifies the location of the MIBS.DATA file	New in CS for OS/390 V2R10
PW_SRC	SNMP agent	Specifies the location of the PW.SRC file	New in CS for OS/390 V2R10
SNMPTRAP_DEST	SNMP agent	Specifies the location of the SNMPTRAP.DEST file	New in CS for OS/390 V2R10
TRAPFWD_CONF	Trap forwarder daemon	Specifies the location of the trap forwarder daemon configuration file.	New in CS for OS/390 V2R10

MIB modules

The following chart provides, at a high level, a description of the network management data objects (known as Management Information Base, or MIB, objects) supported by the SNMP agent and the subagents shipped as part of z/OS. A more formal SNMP definition of the objects supported and the changes in support is provided in the SNMP agent capabilities statement, shipped in the samples directory as /usr/lpp/tcpip/samples/mvstcpip.caps.

Also refer to the appendices of *z/OS Communications Server: IP System Administrator's Commands* for a list of all MIB objects supported.

SNMP agent MIB modules

Table 164. SNMP agent MIB modules

MIB module name	Documented as	Groups supported	Status
SNMP-NOTIFICATION-MIB	RFC 2573	snmpNotifyFilterGroup	New in CS for OS/390 V2R10
SNMP_COMMUNITY		Contains objects for mapping between community-based strings and SNMP message parameters, allows the source address validation on incoming requests, and enables the selection of community strings based on target addresses for outgoing notifications.	New in z/OS CS V1R2

TCP/IP subagent MIB modules

Table 165. TCP/IP subagent MIB modules

MIB module name	Documented as	Groups supported	Status
IBMTCP/IPMVS-MIB	Enterprise specific MIB shipped as /usr/lpp/tcpip/samples/mvstcpip.mi2	Now Supports: ibmTCP/IPmvsSystem Group6 ibmTCP/IPmvsTcpGroup5 ibmTCP/IPmvsUdpGroup3 ibmTCP/IPmvsInterfaces Group4 ibmTCP/IPmvsPortGroup2 ibmTCP/IPmvsAtmSupport Group4 ibmTCP/IPmvsAtmLeGroup2	Changed in CS for OS/390 V2R10. New group replaces: ibmTCP/IPmvsSystemGroup5 ibmTCP/IPmvsTcpGroup4 ibmTCP/IPmvsUdpGroup2 ibmTCP/IPmvsInterfaces Group3 ibmTCP/IPmvsPortGroup ibmTCP/IPmvsAtmSupport Group3 ibmTCP/IPmvsAtmLeGroup
		Documented in the SNMP agent Capability file shipped as /usr/lpp/tcpip/samples/mvstcpip.caps.	Changed in z/OS V1R2
EtherLike-MIB	RFC 2665	etherStatsBaseGroup etherStatsDuplexGroup	New in CS for OS/390 V2R10

Service Level Agreement subagent MIB modules

Table 166. Service Level Agreement subagent MIB modules

MIB module name	Documented as	Groups supported	Status
SLAPM-MIB	RFC 2758 shipped as /usr/lpp/tcpip/samples/slapm.mi2	Now supports slapmBaseGroup2, slapmNotGroup2, slapmEndSystemGroup2, and slapmEndSystemNotGroup2.	Changed in CS for OS/390 V2R10. New groups replace slapmBaseGroup, slapmNotGroup, slapmEndSystemGroup, and slapmEndSystemNotGroup.

z/OS V1R4 Communications Server release summary

This section describes the updates to SNMP introduced in z/OS V1R4 Communications Server.

SNMP agent

The SNMP agent allows you to provide some initial settings for a small set of MIB objects by using the OSNMPD.DATA file. One of the objects for which an initial value can be provided is sysObjectID.0. The sysObjectID.0 object is the vendor's authoritative identification of the network management subsystem contained in the entity. That is, it is intended to uniquely identify the SNMP agent. Changing this value is not recommended and will be disabled in a subsequent release. In z/OS CS V1R4, warning message EZZ63171 will be issued if the object is set by using the OSNMPD.DATA file.

TCP/IP subagent

In z/OS CS V1R4, the TCP/IP subagent supports both IPv4 and IPv6 processing for the TCP scalar counter MIB objects from RFC 2012 and the UDP scalar counter

MIB objects from RFC 2013. Also, some of the outbound ICMP counters were previously only incremented for those ICMP messages that the TCP/IP stack initiated. As of z/OS CS V1R4, all the outbound ICMP counters will now also be incremented for those ICMP messages sent by the TCP/IP stack at the request of an application.

z/OS V1R2 Communications Server release summary

This section describes the updates to SNMP introduced in z/OS V1R2 Communications Server.

SNMP agent

SNMP security enhancements

z/OS V1R2 Communications Server enhances SNMP security for subagents that use TCP to connect to the z/OS CS SNMP agent, instead of using a UNIX connection. This support is provided by a new security product resource name. When this resource name is defined, a subagent will only be allowed to connect to the SNMP agent when the following two conditions are met:

- The subagent is running on the same TCP/IP stack as the SNMP agent.
- The user ID associated with the subagent is permitted to the resource.

Refer to *z/OS Communications Server: IP Configuration Guide* for more information about the new security product resource name.

Restrictions: This function only applies to those SNMP subagents that are using TCP/IP to connect to an SNMP agent, and that are running on the same TCP stack as the agent. Also, this function does not apply to subagents using UNIX to connect to the SNMP agent.

What this change affects:

- Customization
- Installation
- Operations
- Security

Migration procedures: The SNMP security enhancements do not require any action unless you want to take advantage of them. If so, perform the task in the following table.

Table 167. SNMP security enhancements - Migration task

Task	Procedure	Reference
Restrict TCP connection access to the SNMP agent from subagents.	Define the agent's security product resource name, EZB.SNMPAGENT.mvsname.tcpprocname. Ensure that the SERVAUTH class is active and RACLISTed, and that the user IDs under which the SNMP subagents run are permitted to the resource name.	<i>z/OS Communications Server: IP Configuration Guide</i>

SNMP Community MIB

z/OS CS V1R2 includes support of the SNMPv3 Community MIB that allows for the mapping between the community strings and SNMP message parameters. This includes source address validation on incoming requests and community string

selection on outgoing notifications. In addition, the new SNMP community definitions, once provided, can be viewed and changed by SNMP commands.

Restrictions: None.

What this change affects:

- Customization

Migration procedures: The SNMP Community MIB enhancement does not require any action unless you want to take advantage of it. If so, perform the tasks in the following table.

Table 168. SNMP Community MIB enhancement - Migration tasks

Task	Procedure	Reference
Provide new SNMP community definitions that can be viewed and changed by SNMP commands.	Code SNMP_Community statements in SNMPD.CONF file.	<i>z/OS Communications Server: IP Configuration Guide</i> , <i>z/OS Communications Server: IP Configuration Reference</i> , and <i>z/OS Communications Server: IP System Administrator's Commands</i>
If desired, augment the Target Address table to enable a TargetAddress entry to specify multiple addresses and to include the maximum message size.	Update Target_Address statements.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

TCP/IP subagent

z/OS CS V1R2 includes the following enhancements for the TCP/IP subagent:

- Support for Dynamic VIPA management data.
- Support for management data for OSA-Express Gigabit, Fast Ethernet, and ATM155 adapters.
- Support for additional stack TCP and IP statistical counters.
- New MIB objects in the IBM MVS TCP/IP Enterprise-specific MIB:
 - ibmMvsTcpFinwait2Time
 - ibmMvsTcpTimeStamp
 - ibmMvsTcpipSubagentVersion
 - ibmMvsDeviceConfigPackingMode
 - ibmMvsDeviceActualPackingMode
 - ibmMvsTcpConnSndBufSize
 - ibmMvsTcpConnAcceptCount
 - ibmMvsTcpConnExceedBacklog
 - ibmMvsTcpConnCurrBacklog
 - ibmMvsTcpConnMaxBacklog
 - ibmMvsTcpConnWindowScale
 - ibmMvsTcpConnTimeStamp
 - ibmMvsTcpConnServerResourceId
- New ibmTcpipMvsTcpListenerTable in the IBM MVS TCP/IP Enterprise-specific MIB. Each entry represents a TCP connection in Listen state.
- New ibmMvsTcpipSubagentColdStart trap in the IBM MVS TCP/IP Enterprise-specific MIB.

- Obsolete MIB objects from the IBM MVS TCP/IP Enterprise-specific MIB:
 - ibmMvsTcpConnTcpTimer
 - ibmMvsTcpConnTcpSig
 - ibmMvsTcpConnTcpSel
 - ibmMvsTcpConnTcpDet
 - ibmMvsTcpConnTcpPol

Dynamic VIPA MIB enhancements

z/OS V1R2 Communications Server includes the following new MIB objects in the IBM MVS TCP/IP Enterprise-Specific MIB:

- Support is added for dynamic VIPA and Sysplex Distributor management data. Several new MIB tables and traps are defined in the enterprise-specific MIB for this support. Refer to the SNMP chapter of *z/OS Communications Server: IP System Administrator's Commands* for more information.
- Support is added for server (listening) connections. A new `ibmTcpiMvsTcpListenerTable` is created to provide information about every server active on a TCP/IP stack. The entries in this new table will still also be represented in the `tcpConnTable` and the `ibmTcpiMvsTcpConnTable`, except for some load balancing server connections for ports for which SHAREPORT has been specified. Not all of the load balancing servers can be represented in the `tcpConnTable` and the `ibmTcpiMvsTcpConnTable`, but they will all be represented in the new `ibmTcpiMvsTcpListenerTable`.
- An `ibmMvsTcpConnServerResourceId` object is added to the `ibmTcpiMvsTcpConnTable`. It provides the connection ID of the server (listening) connection for each client connection that is connected to a load balancing server.

SNMP OSA-Express MIB enhancements

z/OS V1R2 Communications Server includes new descriptive and performance management data for OSA-Express Gigabit Ethernet, Fast Ethernet, and ATM155 adapters. Since CS for OS/390 V2R5, the SNMP TCP/IP Subagent has supported retrieval of management data from OSA/SF for OSA adapters. In z/OS V1R2 Communications Server, this support is enhanced to provide new tables of management data specifically for OSA-Express adapters. The management data added to the `osafChannelTable` in CS for OS/390 V2R10 for OSA-Express ATM155 adapters is moved to a new OSA-Express channel table, `osaexpChannelTable`. These tables are defined in the IBM MVS TCP/IP Enterprise-specific MIB. Refer to the SNMP chapters in *z/OS Communications Server: IP System Administrator's Commands* and *z/OS Communications Server: IP Configuration Guide* for more information.

SNMP TCP/IP performance counters

z/OS V1R2 Communications Server provides additional statistical counter MIB objects. Several additional TCP and IP protocol layer counters are supported. These can be helpful in problem determination and in general performance analysis of the TCP/IP stack. Also, the following 64-bit interface counter MIB objects from RFC 2233 are now supported:

- ifHCInUcastPkts
- ifHCInMulticastPkts
- ifHCInBroadcastPkts
- ifHCOUcastPkts
- ifHCOUcastMulticastPkts
- ifHCOUcastBroadcastPkts

Restrictions

None.

Dependencies

For the OSA-Express MIB Enhancements, OSA/SF V2R1 must be installed with APAR OW45237 applied in order to retrieve all the OSA-Express management data. The performance MIB object values in the `ibmMvsOsaExpChannelTable`, and all of the MIB object values in the `ibmMvsOsaExpPerfTable`, are only available starting with zSeries z800 and z900 processors where the adapters are at a minimum of microcode level 1.31.

What this change affects

- Customization
- Operations
- Performance
- Usability

Migration procedures

If you want to take advantage of the enhancements for the TCP/IP subagent in z/OS CS V1R2, perform the tasks in the following table.

Table 169. TCP/IP subagent in z/OS CS V1R2 - Migration tasks

Task	Procedure	Reference
Retrieve new OSA-Express management data.	Define OSA-Express adapters to TCP/IP in the profile data set. For OSA-Express ATM155 adapters, retrieve channel data from new <code>osaexpChannelTable</code> instead of existing <code>osafChannelTable</code> .	<i>z/OS Communications Server: IP System Administrator's Commands</i> and <i>z/OS Communications Server: IP Configuration Guide</i>
Use the new MIB objects and traps from network management applications. Stop using the obsolete MIB objects.	The action to take depends on the management application. For the <code>osnmp</code> command, no action is required. For the NetView SNMP command, use the most current copy of the sample <code>MIBDESC.DATA</code> file (shipped in <code>SEZAINST(MIBDESC)</code>). Other management applications may require different changes.	See the appendix that lists the supported MIB objects in <i>z/OS Communications Server: IP User's Guide and Commands</i> . See the agent capabilities statement and enterprise-specific MIB definition for descriptions of MIB objects.

Communications Server for OS/390 V2R10 release summary

This section describes the updates to SNMP introduced in CS for OS/390 V2R10.

SNMP agent

SNMPv3 support was introduced in CS for OS/390 V2R7. CS for OS/390 V2R10 introduces the following enhancements to SNMPv3:

- Support for the use of the UTF-8 character set
- Notification filtering at the source
- Support for informs at the agent
- Encryption support

Additionally, the use of environment variables for `PW.SRC` and `SNMPTRAP.DEST` files is now supported. These enhancements are described in this section.

UTF8 support

UTF8 characters can be used when performing SETs on objects with `SnmpAdminString` syntax. In previous releases, SETs that had non-printable UTF8

characters were rejected; they are now accepted. The fields that have UTF8 characters will be written to the configuration file as printable-hex with a ¢ character preceding it. The ¢ character is reserved to indicate that the field following it is to be considered as containing UTF8 characters.

Restrictions: Because a ¢ character now precedes the UTF8 printable-hex, the ¢ character should not be used as the first character for SnmpAdminStrings. Also, IBM recommends that you do not change the contents of the entries in the configuration file that have a ¢ character preceding them.

What this change affects:

- Usability
- Customization
- Operations

Migration procedures: UTF8 support does not require any action unless any SnmpAdminString variables in the SNMPD.CONF file begin with a ¢ character. If so, perform the task in the following table.

Table 170. UTF8 support - Migration task

Task	Procedure	Reference
Enable support for UTF8 characters in SnmpAdminStrings.	Make sure that the SnmpAdminString names do not start with a ¢ character.	<i>z/OS Communications Server: IP Configuration Reference</i>

Notification filtering support

Notification filtering support at the source is new for CS for OS/390 V2R10 and is an optional part of the SNMPv3 protocols. It allows the ability to select which types of traps or informs are sent to particular managers, reducing network traffic by not sending unneeded notifications.

Restrictions: None.

What this change affects:

- Usability
- Customization
- Operations

Migration procedures: Notification filtering support does not require any action unless filtering of traps and informs by the agent is desired. If so, perform the task in the following table.

Table 171. Notification filtering support - Migration task

Task	Procedure	Reference
Enable notification filtering support at the agent.	Add the required NOTIFY_FILTER _PROFILE and NOTIFY_FILTER statements to the SNMPD.CONF configuration file.	<i>z/OS Communications Server: IP Configuration Reference</i>

Inform support

Inform support at the agent is new for CS for OS/390 V2R10. The SNMP agent can now be configured to send inform type notifications. The receiving management application must be able to confirm receipt of the inform.

Restrictions: None.

What this change affects:

- Usability
- Customization
- Operations

Migration procedures: Inform support does not require any action unless unless informs need to be generated by the agent. If so, perform the task in the following table.

Table 172. Inform support - Migration task

Task	Procedure	Reference
Enable generation of informs at the agent.	Add a NOTIFY statement to the SNMPD.CONF file with snmpNotifyType set to "inform".	<i>z/OS Communications Server: IP Configuration Reference</i>

Encryption support

Encryption support for SNMPv3 requests is now provided as part of the base FMID. In previous releases, a separate feature FMID had to be installed.

Restrictions: None.

What this change affects:

- Customization

Migration procedures: Encryption support does not require any action if you were using the SNMPv3 encryption feature in previous releases. To enable encryption support, perform the task in the following table.

Table 173. Encryption support - Migration task

Task	Procedure	Reference
Define user keys.	Use the pwtokey command to create keys to be entered on the USM_USER statements in the SNMPD.CONF file.	<i>z/OS Communications Server: IP Configuration Reference</i>

Environment variable support

Two new environment variables, PW_SRC and SNMPTRAP_DEST, are added to the SNMP agent. With this support, the location of any SNMP agent configuration file can be configured by using an environment variable.

Restrictions: None.

What this change affects:

- Usability
- Customization
- Operations

Migration procedures: Environment variable support does not require any action unless configuration files need to be read from non-standard places. If so, perform the task in the following table.

Table 174. Environment variable support - Migration task

Task	Procedure	Reference
If desired, change the location from which the PW.SRC and SNMPTRAP.DEST file is read.	Set the PW_SRC and SNMPTRAP_DEST environment variables to point to the desired data set.	<i>z/OS Communications Server: IP Configuration Reference</i>

Allow source VIPA

The SNMP agent is enhanced when SOURCEVIPA is configured so that the SNMP agent can use VIPA addresses as the originating address in packets sent for responses and notifications. In previous releases, the SNMP agent ignored VIPA addresses and caused packets sent by the SNMP agent to contain the physical interface address as the originating address.

Restrictions: None.

Incompatibilities: By default, the SNMP agent now permits the use of VIPA addresses as the source address in packets it originates for responses and notifications. If you are using source VIPA addressing and SNMP, examine your SNMP configurations. If you wish to preserve the pre-CS for OS/390 V2R10 behavior, you may override the default by invoking the SNMP agent with the new -a option.

What this change affects:

- Customization

Migration procedures: Customers using SNMP and source VIPA addressing need to perform one of the tasks in the following table.

Table 175. Allow source VIPA - Migration tasks

Task	Procedure	Reference
If desired, preserve pre-CS for OS/390 V2R10 behavior, where the SNMP agent caused packets it originated to contain the physical interface address.	Invoke OSNMPD with the -a start parameter.	<i>z/OS Communications Server: IP Configuration Reference</i>
If source VIPA addressing is desired with the SNMP agent, verify manager configuration.	Ensure managers that validate packets received from the agent are configured to allow the VIPA address.	<i>z/OS Communications Server: IP Configuration Reference</i>

TCP/IP subagent

CS for OS/390 V2R10 includes the following enhancements for the TCP/IP subagent:

- Support for ATM management data for OSA-Express ATM155 adapters
- Support for the RFC2665 Ethernet MIB for OSA-Express Gigabit and Fast Ethernet QDIO adapters
- ipNetToMediaTable provides Address Resolution Protocol (ARP) Cache information from OSA-Express Gigabit, Fast Ethernet QDIO, and ATM155 QDIO LAN Emulation adapters
- New MIB objects in the IBM MVS TCP/IP Enterprise Specific MIB:
 - ibmMvsAtmLecPortName
 - ibmMvsDevRetryDuration
 - ibmMvsDeviceActualRouterStatus

- ibmMvsLinkArpSupport
- ibmMvsPortBindIpAddr
- ibmMvsPortSAFResource
- ibmMvsPortReuse
- ibmMvsTcpConnDSField
- ibmMvsUdpDSField
- Obsolete MIB objects from the IBM MVS TCP/IP Enterprise Specific MIB:
 - ibmMvsAtmOsasfChannelEcLevel
 - ibmMvsAtmOsasfChannelDate
 - ibmMvsAtmOsasfChanneltime
 - ibmMvsTcpConnIpTos
 - ibmMvsUdpTos

SNMP OSA-Express ATM155 and Ethernet MIB support

In CS for OS/390 V2R5, support was added to the SNMP TCP/IP Subagent to retrieve management data from ATM OSA-2 adapters. In CS for OS/390 V2R10, this support is extended to the OSA-Express ATM155 adapter. All the ATM management data originally provided for ATM OSA-2 will now also be provided for OSA-Express ATM155 except for PVC Create/Delete traps. PVCs cannot be dynamically created/deleted for OSA-Express ATM155. In addition, the CS for OS/390 V2R10 SNMP TCP/IP Subagent supports retrieval of Ethernet MIB data (from RFC 2665) for the OSA-Express Gigabit Ethernet adapter and the OSA-Express Fast Ethernet adapter supporting QDIO. To retrieve the Ethernet MIB data, the OSA adapters must be active to at least one TCP/IP stack on the processor.

As part of these changes, the ATMENABLED parameter was removed from the SACONFIG statement and two new parameters, OSAENABLED and OSADISABLED, were introduced. These new parameters control whether or not the OSA management data can be retrieved. The ATMENABLED parameter will still be accepted and treated as if the new OSAENABLED parameter had been specified.

In addition to these changes, the SNMP TCP/IP Subagent no longer uses the HOSTNAME and HOSTS.SITEINFO information to find the IP address that is used to connect to the SNMP agent. Instead, the Subagent uses the IP address of the LINK interface designated as the primary interface to the stack.

Refer to the SNMP chapter of *z/OS Communications Server: IP Configuration Guide* for details of these configuration changes. Refer to *z/OS Communications Server: IP System Administrator's Commands* for information about the supported SNMP management data.

Restrictions: The OSA/SF V2R1 APARs OW39984 and OW42352 are required in order to obtain the Ethernet MIB and OSA-Express ATM155 management data.

What this change affects:

- Operations
- Customization

Migration procedures: TCP/IP Subagent does not require any action unless you were using changed or obsolete objects from the CS for OS/390 Enterprise Specific MIB, or the TCP/IP Subagent was not using the TCP/IP stack's primary interface IP address to connect to the agent. If so, perform the tasks in the following table.

Table 176. TCP/IP Subagent in CS for OS/390 V2R10 - Migration tasks

Task	Procedure	Reference
Retrieve Ethernet MIB data.	Specify OSAENABLED on SACONFIG statements; define MPCIPA/IPAQENET device/link.	<i>z/OS Communications Server: IP Configuration Reference</i>
Retrieve ATM MIB data for OSA-Express ATM155.	Specify OSAENABLED on SACONFIG statements; define ATM155 as an ATM device/link.	<i>z/OS Communications Server: IP Configuration Reference</i>
Ensure SNMP TCP/IP Subagent connects to SNMP agent.	Verify that stack's primary interface IP address is used for SNMP security.	<i>z/OS Communications Server: IP Configuration Reference</i>
Stop using obsolete MIB objects from network management applications. Use changed syntax for changed objects.	The action to take depends on the network management application. For osnmp, no action is required. For the NetView SNMP command, use the most current copy of the sample MIBDESC.DATA file (shipped in SEZAINST(MIBDESC)). Other management applications may require different changes.	agent capabilities statement and enterprise-specific MIB definition
Use the new MIB objects from network management applications	The action to take depends on the network management application. For osnmp, no action is required. For the NetView SNMP command, use the most current copy of the sample MIBDESC.DATA file (shipped in SEZAINST(MIBDESC)). Other management applications may require different changes.	agent capabilities statement and enterprise-specific MIB definition

OMPRoute subagent

There were no changes in CS for OS/390 V2R10.

Service Level Agreement subagent

See "Policy Agent enhancements" on page 139 for information about CS for OS/390 V2R10 enhancements to the Service Level Agreement Subagent.

osnmp command

Encryption support

Encryption support for SNMPv3 requests is now provided as part of the base FMID. In previous releases, a separate feature FMID had to be installed.

Restrictions: None.

What this change affects:

- Customization

Migration procedures: Encryption support does not require any action if you were using the SNMPv3 encryption feature in previous releases. To enable encryption support, perform the task in the following table.

Table 177. Encryption support - Migration task

Task	Procedure	Reference
Define user keys.	Use the pwtokey command to create keys to be entered on the statements in the OSNMP.CONF file.	<i>z/OS Communications Server: IP Configuration Reference</i>

Environment Variable support

A new environment variable, MIBS_DATA, is added to the osnmp command.

Restrictions: None.

What this change affects:

- Customization
- Usability

Migration procedures: osnmp environment variable support does not require any action unless configuration files need to be read from non-standard places. If so, perform the task in the following table.

Table 178. osnmp environment variable support for CS for OS/390 V2R10 - Migration task

Task	Procedure	Reference
If desired, change the location from which the MIBS_DATA file is read.	Set the MIBS_DATA environment variables to point to the desired data set.	<i>z/OS Communications Server: IP Configuration Reference</i>

Allow source VIPA

The osnmp command is enhanced when SOURCEVIPA is configured so that it can use VIPA addresses as the originating address in packets sent for SNMP requests. In previous releases, the osnmp command ignored VIPA addresses and caused packets sent to contain the physical interface address as the originating address.

Restrictions: None.

Incompatibilities: By default, the osnmp command now permits the use of VIPA addresses as the source address in packets sent for SNMP requests. If you are using source VIPA addressing and SNMP, examine your SNMP configurations. If you wish to preserve the pre-CS for OS/390 V2R10 behavior, you may override the default by invoking the osnmp command with the new -a option or use the NOSVIPA option in the OSNMP.CONF file.

What this change affects:

- Customization

Migration procedures: If you are using SNMP and source VIPA addressing, perform one of the tasks in the following table.

Table 179. osnmp allow source VIPA for CS for OS/390 V2R10 - Migration tasks

Task	Procedure	Reference
If desired, preserve pre-CS for OS/390 V2R10 behavior, where the osnmp command caused packets it originated to contain the physical interface address, for a single command invocation.	Invoke osnmp command with the -a option.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

Table 179. *osnmp allow source VIPA for CS for OS/390 V2R10 - Migration tasks (continued)*

Task	Procedure	Reference
If desired, preserve pre-CS for OS/390 V2R10 behavior, where the <code>osnmp</code> command caused packets it originated to contain the physical interface address, for all commands sent to a particular host.	Configure the NOSVIPA option in the OSNMP.CONF file for the desired agent.	<i>z/OS Communications Server: IP Configuration Reference</i>
If source VIPA addressing is desired with the <code>osnmp</code> command, verify agent configuration.	Ensure SNMP agents are configured to allow the VIPA address. If the agent is the z/OS CS SNMP agent, verify the PW.SRC entries or the COMMUNITY statements in the SNMPD.CONF file allow the use of the VIPA address.	<i>z/OS Communications Server: IP Configuration Reference</i>

NetView SNMP command

No changes in CS for OS/390 V2R10.

SNMP Query Engine

In CS for OS/390 V2R10, if the trap forwarder daemon is started on port 162 and if the SNMP Query Engine will also be used to listen for traps, the SNMP Query Engine should be started on a port other than 162. See “Trap forwarder daemon” on page 248 for more information.

Restrictions

None.

What this change affects

- Operations
- Customization

Migration procedures

SNMP Query Engine does not require any action unless you want to take advantage of this function. If so, perform the task in the following table.

Table 180. *SNMP Query Engine - Migration task*

Task	Procedure	Reference
Allow multiple SNMP managers to monitor for traps at the same IP address.	Start the SNMP Query Engine using the <code>-tp</code> startup option to configure a trap port other than 162. Run the trap forwarder daemon to forward traps from port 162 to the managers monitoring for them.	<i>z/OS Communications Server: IP Configuration Reference</i>

pwtokey command

There were no changes in CS for OS/390 V2R10.

pwchange command

There were no changes in CS for OS/390 V2R10.

Distributed Protocol Interface

There were no changes in CS for OS/390 V2R10.

Trap forwarder daemon

This CS for OS/390 V2R10 function provides a simple trap forwarder daemon to receive a trap on a specified port, typically 162, and to forward it to multiple other ports on the same and/or different hosts. This allows multiple z/OS SNMP managers to be able to receive all the traps sent to one port at a particular IP address. Because only one management application can listen on a port at a particular IP address at a time, it was not previously possible for more than one SNMP manager at an IP address to receive traps sent to the well-known trap port of 162.

Restrictions

The new trap forwarder daemon:

- Listens for trap datagrams from only one port.
- Is not intended to handle informs. If an inform is received, the trap forwarder daemon will treat it as a trap datagram and forward it.
- Does not analyze the received trap datagram; it only forwards it to the specified locations.

What this change affects

- Operations
- Customization

Migration procedures

Trap forwarder daemon does not require any action unless you want to take advantage of this function. If so, perform the tasks in the following table.

Table 181. Trap forwarder daemon - Migration tasks

Task	Procedure	Reference
Ensure that no application other than trapfwd uses the default trap port (162) and start the trap-forwarder daemon on the default trap port (162).	Reserve the port for trapfwd using the PORT statement in the profile data set (hlq.PROFILE.TCPIP).	<i>z/OS Communications Server: IP Configuration Reference</i>
If the trap forwarder daemon needs to be started on port 162 and the SNMP Query Engine process is also required to wait for traps, start the SNMP Query Engine to listen for traps on a port other than 162 and configure the trap forwarder daemon to forward traps to the port on which the SNMP Query Engine is listening.	Use the -tp startup option to specify the port on which the Query Engine should listen for traps.	<i>z/OS Communications Server: IP Configuration Reference</i>

Chapter 12. Migrating to the BIND-based DNS name server

This chapter describes the z/OS UNIX Domain Name System (DNS) name server, which uses the Berkeley Internet Name Domain (BIND) software, the *de facto* standard of the Domain Name System (DNS).

z/OS V1R4 Communications Server BIND 9.2 makes DNS server-to-server and client-to-server IPv6 connections possible; it adds new name server configuration options for IPv6 connections and tuning. BIND 9.2 also provides a new `rndc` utility with a larger set of commands than was available with BIND 9.1. BIND 9.2 `rndc` is not compatible with BIND 9.1 `rndc`.

z/OS CS V1R2 BIND 9.1 was the first implementation of BIND 9 on the z/OS platform, which was a complete rewrite of the name server and associated utilities. This allowed IPv6-type records in zone data. It also introduced better transaction security among servers and clients, as well as zone data authentication capability. It introduced the `rndc` utility to replace and complement UNIX signals for name server local and remote control.

BIND 9 `nsupdate` utility enables client hosts and many DHCP servers to dynamically and securely register their name and address mappings. The z/OS BIND 9 name server is generally compatible with network DHCP servers. The z/OS DHCP server is compatible with the z/OS BIND 4.9.3 name server, but is incompatible with the BIND 9 name server.

Only the z/OS BIND 4.9.3 name server supports DNS/WLM connection balancing. The z/OS Sysplex Distributor function may be used as an alternative to DNS/WLM connection balancing in the absence of the z/OS BIND 4.9.3 name server.

The still available but deprecated z/OS BIND 4.9.3 name server may use Workload Management Services (WLM) to distribute connections among hosts or server applications within a sysplex domain. In that context, a sysplex is a domain that you add to your DNS name space. The z/OS BIND 4.9.3 name server, when coupled with Dynamic Host Configuration Protocol servers with Preboot Execution Environment (DHCP/PXE) support, offers an integrated dynamic update solution, greatly reducing IP address management tasks.

Refer to *z/OS Communications Server: IP Configuration Guide* for details on Dynamic DNS and connection optimization.

This chapter contains new and changed DNS interfaces, including:

- “DNS configuration files” on page 250
- “DNS z/OS UNIX commands” on page 251
- “DNS TSO commands” on page 252
- “DNS environment variables” on page 252

This chapter also contains the following for the BIND-based DNS name server:

- “z/OS V1R4 Communications Server release summary” on page 252
- “z/OS V1R2 Communications Server release summary” on page 256
- “Communications Server for OS/390 V2R10 release summary” on page 262

New and changed interfaces for DNS

This section consists of tables that describe updates that were made for DNS to configuration files, commands, and environment variables. The tables are intended to help you migrate by identifying what is new or changed since your last installation. See “z/OS Communications Server information” on page xxiii to determine which publications you should refer to for complete information about the interfaces, including syntax.

DNS configuration files

Table 182. New or changed configuration files (DNS)

File	Description	Status
BIND DNS domain data file	<p>Name server file containing information about a domain, such as IP addresses and names of hosts in the domain.</p> <p>In CS for OS/390 V2R10, supports DNS SRV RR.</p> <p>In z/OS CS V1R2, zone data files may have new resource records (RRs) for BIND 9 mode. Also, the zone data files for BIND 9 require a \$TTL statement. Each zone must contain at least one NS record for its own domain. If CNAME records are used, no other resource records can exist with that same name, with the exception of SIG, NXT and KEY records for DNSSEC.</p> <p>Also in z/OS CS V1R2, the last field of the SOA record has a different meaning in BIND 9 than in BIND 4.9.3. The last field of the BIND 9 SOA now controls the negative caching TTL instead of supplying the default TTL for the zone, per RFC 2308. The default TTL is now supplied by the \$TTL statement.</p>	Changed in CS for OS/390 V2R10 and z/OS CS V1R2
BIND 9 DNS configuration file (also known as the named.conf file)	<p>In z/OS CS V1R2, this file was used for BIND 9 mode instead of the named.boot file that was used for the BIND 4.9.3 mode. They have a different syntax.</p> <p>Several updates were made in z/OS CS V1R4. See “Configuration file updates” on page 253 for a list of changes.</p>	New in z/OS CS V1R2 and changed in z/OS CS V1R4
rndc.conf file	<p>This file is required only if the rndc command is used. It contains rndc client configuration information. This file does not need to exist on the name server host – only on the client host of the rndc user. Note, however, that the name server to be controlled by rndc has corequisite configuration requirements in the named.conf file.</p> <p>The following changes were made in z/OS CS V1R4:</p> <ul style="list-style-type: none"> • rndc configuration may be done automatically, under the proper circumstances, with the creation of an rndc.key file by the BIND 9 name server. See Table 187 on page 256 for details. • The port and default-port clauses are new to the rndc.conf file. 	New in z/OS CS V1R2; changed in z/OS CS V1R4

DNS z/OS UNIX commands

Table 183. New or changed UNIX commands (DNS)

Command	Description	Status
dig	<p>The domain information groper (dig) is a command line tool that can be used to gather information from the Domain Name System servers.</p> <p>In z/OS CS V1R2, dig may now be run from the UNIX shell. It also has different options than the previous TSO DIG command.</p> <p>In z/OS CS V1R4, the +multiline option was added. This allows control over whether or not records should be displayed in expanded format.</p>	New in z/OS CS V1R2; changed in z/OS CS V1R4
dnssec-keygen	Generates keys for DNSSEC and for TSIG use.	New in z/OS CS V1R2
dnssec-makekeyset	Used to create a key set from one or more keys when configuring DNSSEC.	New in z/OS CS V1R2
dnssec-signkey	Used to sign one child's keyset with the parent zone's private key when configuring DNSSEC.	New in z/OS CS V1R2
dnssec-signzone	Used to sign zones with the keys generated by dnskeygen when configuring DNSSEC.	New in z/OS CS V1R2
dnsmigrate	Migration aid that converts named.boot files for the BIND 4.9.3 mode into named.conf files suitable for the BIND 9 mode.	New in z/OS CS V1R2
named	<p>Starts the BIND DNS name server for either BIND 4.9.3 mode or BIND 9 mode.</p> <p>In z/OS CS V1R2, named has new options in BIND 9 mode.</p>	Changed in z/OS CS V1R2
nslookup	Synonym for onslookup.	Changed in CS for OS/390 V2R10 and z/OS CS V1R2
nsupdate	<p>Creates and executes DNS update operations on a host record. Runs in BIND 4.9.3 mode or BIND 9 mode.</p> <p>In z/OS CS V1R2, nsupdate has new options in BIND 9 mode.</p>	Changed in z/OS CS V1R2
onslookup	<p>Queries domain name servers. Runs in BIND 4.9.3 mode or BIND 9 mode.</p> <p>In CS for OS/390 V2R10, onslookup supports DNS SRV RR.</p> <p>In z/OS CS V1R2, onslookup has new options in BIND 9 mode.</p>	Changed in CS for OS/390 V2R10

Table 183. New or changed UNIX commands (DNS) (continued)

Command	Description	Status
rndc	<p>Remote Name Daemon Control (rndc) is a tool that allows the system administrator some degree of control over the BIND 9 name server.</p> <p>The following updates were made in z/OS CS V1R4:</p> <ul style="list-style-type: none"> • A V1R4 BIND 9 name server cannot be used with a V1R2 rndc client, nor can it be used with an rndc client on a non-z/OS platform that is from a version of BIND prior to BIND 9.2.0. Similarly, the V1R4 rndc client cannot be used with a V1R2 BIND 9 name server, nor can it be used with a BIND name server on a non-z/OS platform that is older than BIND 9.2.0. • The rndc status command is new. It displays the status of the server. • The rndc flush command is new. It flushes the server's cache. • The rndc reconfig command is new. It reloads the configuration file and any new zone files, but does not reload existing zone files. • The rndc trace and notrace commands are new. They allow control of the name server debugging level. 	New in z/OS CS V1R2 and changed in z/OS CS V1R4
rndc-confgen	Generates configuration files for rndc.	New for z/OS CS V1R4

DNS TSO commands

Table 184. New or changed TSO commands (DNS)

Command	Description	Status
nslookup	<p>Queries the DNS name server.</p> <p>In CS for OS/390 V2R10, nslookup supports DNS SRV RR.</p>	Changed in CS for OS/390 V2R10

DNS environment variables

The following table includes the environment variable that was new for DNS in z/OS CS V1R2. The table does not include any environment variables that were introduced prior to z/OS CS V1R2.

Note: There were no new or changed environment variables for DNS in z/OS CS V1R4.

Table 185. Environment variables (DNS)

Environment variable	Description	Status
DNS_VERSION	Specifies the default version for named, nslookup, and nsupdate. Values can be 'v4' or 'v9'.	New in z/OS CS V1R2

z/OS V1R4 Communications Server release summary

The BIND 9 name server was introduced in z/OS V1R2 CS; see "BIND DNS upgrade" on page 256 for details. In z/OS CS V1R4, the BIND 9 name server is upgraded to the BIND 9.2 level. This allows DNS communications from server-to-server and from client- (utilities and resolvers) to-server over IPv6 connections, with additional configuration options relating to IPv6 connections and

server tuning. The z/OS CS V1R2 version of the name server supported IPv6 resource records, but was unable to communicate over IPv6.

With BIND 9.2, resolvers are able to receive complete and accurate DNS responses for some types of IPv6 queries because BIND 9.2 includes support for A6 and DNAME chaining on behalf of resolvers that do not support such chaining. Note that BIND 9.1 did not support resolution of resource record through record chaining on behalf of a resolver.

For more information on A6 chaining, see the section that discusses address lookups using A6 records in *z/OS Communications Server: IP Configuration Guide*.

Configuration file updates

BIND 9 DNS configuration file (named.conf)

The following updates were made to the BIND 9 DNS configuration file (named.conf) in z/OS CS V1R4:

- The unmatched category has been added to the logging{} statement.
- The forwarders option now accepts an optional port.
- The allow-v6-synthesis option was added to the options{} statement and view statements.
- The serial-query-rate option was added to the options{} statement.
- The random-device option was added to the options{} statement.
- The max-cache-size option was added to the options{} statement.
- The minimal-responses option was added to the options{} statement.
- The listen-on-v6 option was added to the options{} statement.
- The query-source-v6 option was added to the options{} statement.
- The transfer-source-v6 option was added to the options{} and zone{} statements.
- The notify-source-v6 option was added to the options{} and zone{} statements.
- The max-buffered-messages option was added to the options{} statement.
- The match-mapped-addresses option was added to the options{} statement.
- The edns option was added to the server{} statement.
- The \$GENERATE directive now supports DNAME records.
- The behavior of the controls{} statement has changed. rndc may be used without a controls{} statement under the proper circumstances. Also, the keys clause of the controls{} statement is now optional.
- Root hints are now fully optional. For class IN views, a compiled-in hints file will be used by default. For non-IN class views, there is no compiled-in default hints file and such views can provide authoritative services, but not recursion.
- ACL names are no longer case sensitive.
- Configuration files no longer have reserved words.
- The default TTL for BIND 9 zones has changed. BIND 9 strictly complies with the RFC 1035 and RFC 2308 rules regarding omitted TTLs in zone files. Omitted TTLs are replaced by the value specified with the \$TTL directive, or by the previous explicit TTL if there is no \$TTL directive.

If there is no \$TTL directive and the first RR in the file does not have an explicit TTL field, the zone file is illegal according to RFC 1035 because the TTL of the first RR is undefined. Unfortunately, BIND 4 and many versions of BIND 8 accept such files without warning and use the value of the SOA MINTTL field as a default for missing TTL values. The BIND 9 name server in z/OS CS V1R2 did not load such files. The BIND 9 name server in z/OS CS V1R4 emulates the

nonstandard BIND 4/8 SOA MINTTL behavior and loads the files (provided that the SOA is the first record in the file), but will issue the warning message "no TTL specified; using SOA MINTTL instead".

To avoid problems, IBM recommends that you use a \$TTL directive in each zone file.

- The BIND 9 name server logging has changed slightly. If the logging level is chosen as 'debug' and the debug level is omitted, the default debug level is now 1 instead of 0.
- When a size limit is associated with a log file, it will only be rolled when the size is reached, not every time the log file is opened. For example, the log files will no longer be automatically rolled if the name server is stopped and restarted.
- Options that accepted IPv4 addresses now also accept IPv6 addresses.
- Prior to z/OS CS V1R4, some options that were inappropriate for a given type of zone were ignored. As of z/OS CS V1R4, these types of errors are no longer ignored and they cause an error message to be issued and the name server to end. Refer to the table for named.conf options and valid zone types in *z/OS Communications Server: IP Configuration Reference*. It lists the options that will undergo this enforcement and lists the types of zones for which they are valid.
- The print-category, print-severity, and print-time logging options have had their default value changed from *no* to *yes*.
- The print-threadid logging option is new.

rndc.conf configuration file

The following changes were made to the rndc.conf configuration file in z/OS CS V1R4:

- rndc configuration may be done automatically, under the proper circumstances, with the creation of a rndc.key file by the BIND 9 name server. See Table 187 on page 256 for details.
- The port and default-port clauses are new to the rndc.conf file.

See "DNS configuration files" on page 250 for more information about changes to configuration files.

UNIX command updates

Updates were made to the following UNIX commands in z/OS CS V1R4 for DNS:

- dig
- named
- rndc

In addition, a new UNIX command was introduced in z/OS CS V1R4 for DNS:

- rndc-confgen

See "DNS z/OS UNIX commands" on page 251 for details about all updates to UNIX commands for DNS.

Dependencies

In order for the BIND 9 name server to perform A6 chain resolution for DNS A6 resource records on behalf of resolvers that do not support A6 chain resolution, the BIND 9 name server must be configured with the *allow-v6-synthesis* option in named.conf.

Restrictions

None.

What this change affects

- Customization
- Diagnosis
- Operations
- Performance
- Storage

Migration procedures

If you want to run the name server using the BIND 9.2 upgrades, perform the tasks in the following table.

Table 186. BIND 9.2 upgrades - Migration tasks

Task	Procedure	Reference
Allow the name server to communicate over IPv6 (optional).	Specify the <i>listen-on-v6</i> option in <i>named.conf</i> . You may also specify IPv6 addresses in access control lists, server statements, masters clause in slave zone statement, and any other options that specify IP addresses.	<i>z/OS Communications Server: IP Configuration Reference</i>
Add IPv6 information to the name server (optional).	Add IPv6 records and/or zones to the name server configuration file and/or existing zone files.	<i>z/OS Communications Server: IPv6 Network and Application Design Guide</i>
Enable A6 Chain Resolution for Resolvers that are unable to perform A6 Chain Resolution on their own. (optional).	Specify the <i>allow-v6-synthesis</i> option in the <i>named.conf</i> file. Specify the addresses of the resolvers this option will apply to in the Access Control List (ACL).	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Limit cache storage size if desired. (optional).	Specify the <i>max-cache-size</i> option in the <i>named.conf</i> file.	<i>z/OS Communications Server: IP Configuration Reference</i>
Ensure syslogd is running.	Start the Syslog Daemon.	<i>z/OS Communications Server: IP Configuration Guide</i>
Start the BIND 9 name server with the new options.	Start the BIND 9 name server start procedure or start from the z/OS UNIX shell with the <i>named</i> command.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Check for errors.	Check the syslog output file and <i>named</i> log files for errors or warnings. Query the name server with <i>dig</i> or <i>nslookup</i> to further test the name server configuration.	<i>z/OS Communications Server: IP Diagnosis</i> , <i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i> , and <i>z/OS Communications Server: IP System Administrator's Commands</i>
Be aware that updates were made to the BIND 9 DNS configuration file (<i>named.conf</i>). For example, the default TTL for BIND 9 zones has changed.	See "Configuration file updates" on page 253 for details of changes. To avoid problems in BIND 9 zones, you should use a <i>\$TTL</i> directive in each zone file.	<i>z/OS Communications Server: IP Configuration Reference</i>

Automatic rndc configuration for a local rndc client

In order to allow automatic configuration of a local rndc client for the BIND9 name server, perform the tasks in the following table.

Note: This will prevent remote rndc client control of the BIND9 name server.

Table 187. IPv6 DNS - Migration tasks for automatic rndc configuration for a local rndc client

Task	Procedure	Reference
Disable any existing rndc configuration.	Do the following: 1. Remove any control statements from named.conf. 2. Remove /etc/rndc.conf if it exists.	<i>z/OS Communications Server: IP Configuration Reference</i>
Create the /etc/rndc.key file.	Run rndc-confgen with the -a option	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Allow the name server to read the /etc/rndc.key file and create the dynamic control channel for rndc.	Stop and restart the BIND9 name server.	<i>z/OS Communications Server: IP System Administrator's Commands</i>
Locally control the BIND9 name server.	Issue rndc commands to a local BIND9 name server.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

z/OS V1R2 Communications Server release summary

BIND DNS upgrade

z/OS V1R2 Communications Server provides a port of the BIND-based version 9 name server to the zSeries platform. It is known as the BIND 9-based name server and it is different from the BIND 4.9.3-based name server that existed in previous CS for OS/390 releases. Both modes of the name server are available through one command interface. The BIND 9 mode of the name server allows for greater security, has IPv6 support, and brings an industry standard Dynamic DNS (DDNS) to the zSeries platform. However, when run in the BIND 9 mode, the name server does not have DNS/WLM capability nor is it compatible with prior CS for OS/390 Dynamic DNS (DDNS) support.

In a multiple stack (Common INET) environment, the BIND 9 name server is a generic server which does not have stack affinity. This is in contrast to the BIND 4.9.3 name server which does have stack affinity. Refer to the discussion of Multiple TCP/IP Stack (Common INET) Considerations in *z/OS Communications Server: IP Configuration Guide* for implications of this behavior.

The TSO NSLOOKUP tstamp option/subcommand is not available. Any user automation which depends on TSO NSLOOKUP timestamps in the output will be affected.

In z/OS V1R2 Communications Server, there are three different ways to run your name server:

- In BIND 9 mode only
- In BIND 4.9.3 only
- In both BIND 9 and BIND 4.9.3 mode

All three ways are discussed in this section. Read each section and determine the best scenario for your installation.

Running the name server in BIND 9 mode only

When running the name server in BIND 9 mode only, industry standard DDNS is supported. IPv6 support is also supported, and security is enhanced. Since BIND 9 does not support DNS/WLM connection balancing, Sysplex Distributor may be used instead for sysplex load balancing.

The `named.boot` file in the BIND 4.9.3-based DNS server is replaced with the `named.conf` file for BIND 9-based DNS servers. Along with the name change is a change in syntax. A migration tool (initiated by specifying a new UNIX command called `dnsmigrate`) is supplied to convert the files from the BIND 4.9.3-based DNS format to the newer BIND 9-based DNS format. The migration tool will not do backwards conversion from the newer version to the older version.

DNS performance issues: In general, the BIND 9 name server may perform slower than the BIND 4.9.3 name server for small zones on simple query/response operations, or you may achieve equivalent throughput as a BIND 4.9.3 name server but with higher CPU consumption, depending on if your system is already CPU constrained. The BIND 9 name server contains extra overhead to support multi-threading, and DNSSEC. For small zones, the extra overhead for multi-threading may cause a performance disadvantage. On the other hand, the multi-threading may improve performance for large zones.

BIND 4.9.3 name servers are unable to answer queries for a period of time during zone transfers. The larger the zone, the more noticeable this may become. Because of the multi-threading, BIND 9 name servers, in contrast, are able to answer queries during zone transfers. Furthermore, BIND 9 name servers are capable of Incremental Zone Transfers, while BIND 4.9.3 name servers are not. Incremental Zone Transfer allows only the changed information in a zone to be sent to slave name servers instead of the entire zone. If your name servers employ dynamic update and change frequently, the Incremental Zone Transfer feature of BIND 9 may offer some performance advantages while reducing network traffic. The use of DNSSEC (authenticating DNS data by using digital signatures) will also have a performance cost. Not only will the authentication process require more CPU, but signing a zone greatly increases the zone's size. This has further ramifications. DNS message sizes will increase between client and server, and between DNS servers. If the message size becomes too large for UDP, the message will be sent by TCP, which is more resource intensive.

Because the BIND 9 name server is multi-threaded, it can take advantage of any additional processors you add to the system. The BIND 9 name server will detect the number of logical CPUs configured for the system (if not running partitioned) or LPAR (if running partitioned), and create additional worker threads accordingly. For relatively simply configured name servers which are small, not using DNSSEC, or are not kept busy, the overhead in managing the extra threads created on a multiprocessor image may actually be disadvantageous. If you feel this may be the case, you can override the number of worker threads created by using the `'-n'` option when starting the name server. The number of logical CPUs detected (and therefore, the number of worker threads created by default) is logged when the name server is started.

Requirements when running the name server in BIND 9 mode only: The following are required when running the name server in BIND 9 mode only:

- Name servers running in the BIND 9 mode must use the `named.conf` file with the `named.conf` syntax.
- BIND 9 zone data files require a `$TTL` statement even though the syntax for zone data files remains the same as they were in BIND 4.9.3

- BIND 9 name servers must specify one-answer transfer format if serving as a master to a BIND 4.9.3 name server. Many-answers is the default.
- BIND 9 name servers must specify one-answer transfer format if users will be asking for zone transfers (by using the `ls -d` subcommand) from pre-BIND 9 versions of `nslookup`.
- A BIND 9 version of `nsupdate` must be used when updating a BIND 9 DNS server.

Restrictions when running the name server in BIND 9 mode only: The following restrictions or incompatibilities apply when running the name server in BIND 9 mode only:

- DNS/WLM (Sysplex Connection balancing) cannot be done by a name server running in BIND 9 mode
- z/OS CS DHCP servers or OS/2[®] DHCP servers cannot update a BIND 9 name server.
- The BIND 9 name server is a generic server, unlike the BIND 4.9.3 name server which has stack affinity. If stack affinity is desired for the BIND 9 name server, use the `_BPXK_SETIBMOPT_TRANSPORT` environment variable.
- There is a potential migration or coexistence problem on zone transfers when the master (primary) name server is a BIND 9-based DNS name server and the slave (secondary) name server is a BIND 4.9.3-based DNS name server, or any other name server running on another platform that does not support the many-answers zone transfer format. If any slave name servers fit into this category and the master name server is a BIND 9-based DNS name server, the BIND 9-based DNS name server must use the 'one-answer' transfer format. Many-answers is the default.
- A BIND 4.9.3 name server cannot be a slave to a BIND 9 name server if the BIND 9 name server contains any Resource Records (RRs) that the BIND 4.9.3 name server does not understand.
- A BIND 9 name server cannot be a slave (secondary) to any earlier version of a name server, including BIND 4.9.3, if the master (primary) contains CNAME resource records and other types of resource records with the same name as the CNAME resource records. An error message will be generated related to 'multiple RRs of singleton type', in this case.
- A BIND 9 name server cannot be a slave (secondary) to any earlier version of a name server, including BIND 4.9.3, if the master (primary) does not contain NS records for its own zone.
- A BIND 9 name server zone file must contain NS records for its own zone. Previous versions of DNS did not require this.
- A BIND 9 name server zone file may not contain CNAME resource records and other types of resource records with the same name as the CNAME resource records, with the exception of SIG, NXT, and KEY resource records when used for DNSSEC. Previous versions of DNS allowed this.
- The `dnsmigrate` tool has the following restrictions:
 - A maximum string length of 256 characters
 - A maximum line length of 512 characters
 - A maximum of 100 comments (whole- or partial-line)
 - A maximum of 1000 zones (of all types)
 - A maximum of 50 include statements
 - A maximum of 32 IP addresses or subnets for those directives that use IP lists (such as `secondary`, `forwarders`, `xfrnets`, and so on)

Migration procedures: If you want to run the name server in BIND 9 mode only, perform the tasks in the following table.

Table 188. Running the name server in BIND 9 mode only - Migration tasks

Task	Procedure	Reference
Convert named.boot file syntax (for BIND 4.9.3) to named.conf format (for BIND 9)	Run the dnsmigrate tool on the named.boot file.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Reserve ports (optional).	Optionally reserve port 53 for UDP and TCP for named. If you are starting named from a proc, the name to use on the PORT statement is the proc name with a suffix of 1. For example, specify NAMED1 if the name of the proc is NAMED. You can also reserve ports by using the name OMVS. If started from z/OS UNIX, port reservation is also optional. If you decide to reserve ports, you must reserve the ports by using the name OMVS.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Update zone data files.	Perform the following steps: 1. Add a \$TTL statement to the top of each zone data file. 2. Ensure that each zone contains at least one NS record for its own domain. 3. If CNAME records exist in the zone data file, ensure that no other resource records exist with that same name.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Enable new BIND 9 features in the name server.	<ul style="list-style-type: none"> • Add options and directives to the named.conf file. • Optionally, generate and deploy keys for DNSSEC and TSIG. • Optionally, sign the appropriate zones with the zone key. 	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Configure logging.	Add the logging statement to the named.conf file.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Start the name server in BIND 9 mode.	Use the -V named start option, or use the 'DNS_VERSION' environment variable.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>
Resolve configuration errors that may occur implementing the new BIND 9 features.	Follow instructions within error messages that might display in syslog or the console. Enable tracing to the debug file.	<i>z/OS Communications Server: IP Configuration Guide</i> , <i>z/OS Communications Server: IP Configuration Reference</i> , and <i>z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)</i>

Running the name server in BIND 4.9.3 mode only

When running the name server in BIND 4.9.3 mode only, you have DNS/WLM capability and the name server is compatible with previous CS for OS/390 Dynamic DNS (DDNS).

Note: When running NAMED in BIND 4.9.3 mode, you will see a step with a Condition Code of 1, for example, OMVSEX COND CODE=0001. This is a normal occurrence. In addition, you will see the following message:

```
EZZ6475I NAMED:  READY TO ANSWER QUERIES.
```

This means that NAMED is running.

Requirements when running the name server in BIND 4.9.3 mode only: The following are required when running the name server in BIND 4.9.3 mode only:

- Name servers running in BIND 4.9.3 mode must use the traditional named.boot file with the named.boot syntax.
- BIND 9 name servers must specify one-answer format if serving as a master to a BIND 4.9.3 name server. Many-answers is the default.
- The BIND 4.9.3 version of nsupdate must be used when updating a BIND 4.9.3 DNS server.
- If the TCPIP Profile reserves port 53 for the name server, and you do not reserve port 53 using the name OMVS, you must update the name on the port 53 port reservation statements. The name to reserve for port 53 is now the name server proc name with a suffix of 2 instead of the former suffix of 1. For example, PORT 53 UDP NAMED1 should be changed to PORT 53 UDP NAMED2. The same change is needed for the TCP port reservation.

Restrictions when running the name server in BIND 4.9.3 mode only: The following restrictions or incompatibilities apply when running the name server in BIND 4.9.3 mode only:

- You cannot dynamically update a BIND 4.9.3 name server by nsupdate when nsupdate is operated in BIND 9 mode.
- Incremental Zone Transfer (IXFR) is not supported.
- You cannot dynamically update a BIND 9 name server by nsupdate when nsupdate is operated in BIND 4.9.3 mode.
- Name servers running in BIND 4.9.3 cannot understand the many-answers zone transfer format that more advanced name servers (including BIND 9 mode) are capable of supporting.
- CS for OS/390 DHCP servers and OS/2 DHCP servers may only update a BIND 4.9.3 name server.
- IPv6 resource records are not supported by a BIND 4.9.3 name server.
- NOTIFY (which is used to tell a slave that the master has changed) is not supported by a BIND 4.9.3 name server.
- DNSSEC Security is not available in BIND 4.9.3 mode.
- TSIG Security is not available in BIND 4.9.3 mode.
- Access Control List (ACL) Security is not available in BIND 4.9.3 mode.
- A BIND 4.9.3 name server will pass information that contains RRs it does not understand back to a client or nameserver that queried it. However, it may not cache that information. This permits a BIND 4.9.3 name server to do recursive queries for RRs it does not understand.

Migration procedures: If you want to run the name server in 4.9.3 mode only, perform the task in the following table.

Table 189. Running the name server in 4.9.3 mode only - Migration task

Task	Procedure	Reference
Update the name on the port 53 port reservation statements and on the TCP port reservation, if necessary.	If the TCPIP Profile reserves port 53 for the name server, and you do not reserve port 53 using the name OMVS, you must update the name on the port 53 port reservation statements. The name to reserve for port 53 is now the named proc name with a suffix of 2 instead of the former suffix of 1. For example, PORT 53 UDP NAMED1 should be changed to PORT 53 UDP NAMED2. The same change is needed for the TCP port reservation.	<i>z/OS Communications Server: IP Configuration Guide</i> and <i>z/OS Communications Server: IP Configuration Reference</i>

Running the name server in BIND 9 mode and BIND 4.9.3 mode simultaneously

Because each name server version supports some functions that the other does not, you may wish to run both name servers on the same TCP/IP stack. This is accomplished by having each name server listen on a different set of interfaces.

When running the name server in both BIND 9 and BIND 4.9.3 modes, the same requirements and restrictions of running them separately apply. See “Running the name server in BIND 9 mode only” on page 257 and “Running the name server in BIND 4.9.3 mode only” on page 259 for details.

Migration procedures: If you want to run the name server in BIND 9 mode and BIND 4.9.3 mode simultaneously, perform the tasks in the following table.

Table 190. Running the name server in BIND 9 mode and BIND 4.9.3 mode simultaneously - Migration tasks

Task	Procedure	Reference
Allow the name server port (53) to be shared.	Remove any PORT reservations for port 53 or else reserve PORT 53 for TCP for both jobnames. Ensure that PORT 53 TCP port reservations have a suffix of 2 for BIND 4.9.3 and a suffix of 1 for BIND 9 if they are started from a proc. For example, specify one of the following: PORT 53 TCP NAMED2 ;BIND 4.9.3 PORT 53 TCP NAMED1 ;BIND 9 Note: UDP PORT reservation for multiple jobnames is not allowed.	<i>z/OS Communications Server: IP Configuration Reference</i>
Bind each name server to its own set of IP interfaces.	<ol style="list-style-type: none"> 1. Bind the BIND 9 name server to the set of interfaces you wish to be serviced by the BIND 9 name server using the 'listen-on{' option in the named.conf file. 2. Bind the BIND 4.9.3 name server to the interface you wish to be serviced by the BIND 4.9.3 name server using the BIND option on the PORT statement in the TCPIP.PROFILE for the name server's port. This should use the job name of the BIND 4.9.3 name server. 	<i>z/OS Communications Server: IP Configuration Reference</i>
Assign unique job names to the two name servers and correlate those names with the job names used in the previous steps.	Ensure that the jobnames match those on the PORT statement, with the exception of the numerical suffix. Port reservation will not work if named is started from z/OS UNIX, unless the ports are reserved with the name OMVS.	<i>z/OS Communications Server: IP Configuration Guide</i>

Table 190. Running the name server in BIND 9 mode and BIND 4.9.3 mode simultaneously - Migration tasks (continued)

Task	Procedure	Reference
Store the name server process IDs (PIDs) in unique files.	Configure the BIND 9 name server to store the process ID (PID) in a file other than that one used for the BIND 4.9.3 name server (/etc/named.pid). This is done with the 'pid-file' named.conf file option.	<i>z/OS Communications Server: IP Configuration Reference</i>

DNS SRV Resource Record support upgrade

DNS SRV Resource Record support for BIND 4.9.3 was introduced in CS for OS/390 V2R10; see “DNS SRV Resource Record support” for details. In z/OS V1R2 Communications Server, DNS SRV RRs is also supported by BIND 9. Windows 2000 is the most common network component that uses SRV records. BIND 9 fully supports non-secure dynamic update and is a better choice over BIND 4.9.3 if Windows 2000 will be updating your name server.

The same restrictions and migrating procedures mentioned in the CS for OS/390 V2R10 section, “DNS SRV Resource Record support”, apply when using BIND 9.

DNS non-swappable mode support

DNS non-swappable mode support for BIND 4.9.3 was introduced in CS for OS/390 V2R10; see “DNS non-swappable mode support” on page 263 for details. In z/OS V1R2 Communications Server, DNS non-swappable mode is also supported by BIND 9.

The same restrictions and migrating procedures mentioned in the CS for OS/390 V2R10 section, “DNS non-swappable mode support” on page 263, apply when using BIND 9.

Communications Server for OS/390 V2R10 release summary

DNS SRV Resource Record support

In CS for OS/390 V2R10, the z/OS UNIX DNS BIND 4.9.3 name server is enhanced to allow resource records (RRs) of the SRV type. This support was added primarily to allow DNS compatibility with Windows 2000 machines that utilize these types of resource records. This support is available in CS for OS/390 V2R6, CS for OS/390 V2R7, and CS for OS/390 V2R8 by using APAR PQ36653.

Restrictions

DNS servers that do not support SRV resource records cannot be secondary (slave) name servers to DNS servers that contain SRV resource records. This includes DNS name servers running on releases CS for OS/390 V2R6 and later if APAR PQ36653 is not applied, as well as releases prior to CS for OS/390 V2R6.

What this change affects

- Usability

Migration procedures

If you want to take advantage of the DNS SRV RR support, perform the tasks in the following table.

Table 191. DNS SRV RR support - Migration tasks

Task	Procedure	Reference
Understand which SRV records may be needed by hosts in domains administered by your DNS server.	Examine hosts/machines that may attempt to dynamically create SRV records in domains administered by your DNS server.	
Add the SRV records and any related A and PTR records to your DNS data files.	Edit the DNS forward domain data files with the SRV and related A records, and optionally edit the DNS reverse domain data files.	<i>z/OS Communications Server: IP Configuration Reference</i>
Reload the DNS data with the new data files.	Issue the sigHUP signal to the name server or stop and re-start the name server.	<i>z/OS Communications Server: IP Configuration Reference</i>
Test the new name server configuration.	Use the TSO or UNIX 'nslookup' command to query SRV records in the affected domain.	<i>z/OS Communications Server: IP System Administrator's Commands</i>

DNS non-swappable mode support

In CS for OS/390 V2R10, the DNS BIND 4.9.3 name server can be made to run in a non-swappable state.

Restrictions

CS for OS/390 V2R6, CS for OS/390 V2R7, and CS for OS/390 V2R8 users are required to have APAR PQ36653 in order to use this function.

What this change affects

- Performance

Migration procedures

If you want to take advantage of the DNS non-swappable mode support, perform the tasks in the following table.

Table 192. DNS non-swappable mode support - Migration tasks

Task	Procedure	Reference
Make the name server run in a non-swappable state.	Configure RACF to allow the name server to run as non-swappable.	<i>z/OS Communications Server: IP Configuration Guide, /EZARACF Sample</i>
Make the name server run in a swappable state.	Configure RACF to allow the name server to run as swappable.	<i>z/OS Communications Server: IP Configuration Guide, /EZARACF Sample</i>

Appendix A. Migrating from Community-Based Security to SNMPv3

To use the enhanced message security and access control of SNMPv3, you need to migrate your configuration from the legacy PW.SRC and SNMPTRAP.DEST configuration files used by the SNMP agent to new entries in the SNMPD.CONF configuration file. (If you used community-based security and do not need enhanced security, you do not need to make any changes.) Additional entries are also required in the configuration file for the osnmp command.

Migrating the SNMP agent (osnmpd) configuration

Before migrating legacy configuration files to the SNMPD.CONF file, read the *z/OS Communications Server: IP Configuration Reference* to learn which default configuration entries can be provided by the DEFAULT_SECURITY statement. Doing so may reduce the number of configuration entries you need to define.

Migrating SNMP community entries from PW.SRC

Entries in the PW.SRC file need to be converted to SNMP COMMUNITY entries in the SNMPD.CONF file. Because the View-based Access Control Model (VACM) is applied also to SNMP community entries in the SNMPD.CONF file, appropriate group, view and access definitions are needed. Additional configuration statements are required to produce an equivalent configuration to what had been defined in the PW.SRC file.

Because VACM is applied to SNMP COMMUNITY entries, you can choose to use only the powerful access control features of SNMPv3 without the message level security. In other words, you can configure the SNMP agent so that only particular MIB objects can be read or written using a specified community name.

To migrate community entries, follow the steps below:

1. For each community name defined in the PW.SRC file, create an SNMP COMMUNITY statement in the SNMPD.CONF file. The community name should be used in the communityName field as well as in the securityName field. Use the network mask in the netMask field and the network in the netAddr field.
If authentication on a target address is desired, the TransportTag value should be included in the connection with the TagList value in the TargetAddress statement. The optional keywords tMask and tMMS can also be used on this statement.
2. Define one or more VACM_VIEW entries to specify groups of MIB objects to be read or written using a particular community name. You can use a community name to access all MIB objects or particular sets of MIB objects. For each set of objects for which access is to be permitted, define a VACM_VIEW entry.
3. For each SNMP COMMUNITY entry, create a VACM_GROUP entry that identifies the securityName specified on the COMMUNITY entry as a member of a group. If different MIB objects are to be accessible to different community names, define more than one group. Otherwise, all VACM_GROUP statements may specify the same group.

Note: Because the VACM_GROUP statement requires a securityModel field, you must define two VACM_GROUP statements for a community name that is to be used for both SNMPv1 and SNMPv2c requests.

4. Define VACM_ACCESS statements for each group to identify the views that are to be used by a group for reading, writing, and receipt of notification (trap) data.

The following examples show how to migrate an entry from the PW.SRC file to the SNMPD.CONF file:

- PW.SRC entry


```
passwd1 9.0.0.0 255.0.0.0
```
- SNMPD.CONF entries


```
SNMP COMMUNITY passwd1 passwd1 noAuthNoPriv 9.0.0.0 255.0.0.0
VACM_VIEW bigView internet - included -
VACM_GROUP group1 SNMPv1 passwd1
VACM_ACCESS group1 - - noAuthNoPriv SNMPv1 bigView bigView bigView -
```

Migrating trap destination entries from SNMPTRAP.DEST

SNMPv3 notification processing lets you define exactly which security parameters should be used when the SNMP agent sends notifications of asynchronous events. In order to configure the SNMP agent to send notifications with SNMPv3, the entries in the legacy SNMPTRAP.DEST file need to be converted to entries in the SNMPD.CONF file.

To migrate trap destination entries, follow these steps:

1. Define at least one NOTIFY entry to indicate that trap-type notifications are to be sent.

Note:

The SNMP agent on z/OS CS does not currently support the generation of inform-type notifications.

2. For each entry in the SNMPTRAP.DEST file, configure a TARGET_ADDRESS statement in the SNMPD.CONF file. Use the IP address to which the notification is to be sent as the value for the tAddress field.
3. You can have all traps sent with the same security parameters (for example, community name with an SNMPv1 trap format) to all trap destinations, or you can define different security parameters to be used for different destinations. For each set of security parameters to be used, define a TARGET_PARAMETERS statement. Enter the paramsName field from the TARGET_PARAMETERS statement in the targetParams field on all TARGET_ADDRESS statements for which those security parameters are to be used.

The following examples show how to migrate trap destination entries from the SNMPTRAP.DEST file to the SNMPD.CONF file:

- SNMPTRAP.DEST entry


```
9.67.113.79 UDP
```
- SNMPD.CONF entry


```
NOTIFY notify 1 traptag trap -
TARGET_ADDRESS Target1 UDP 9.67.113.79 traptag trapparms1 - - -
TARGET_PARAMETERS trapparms1 SNMPv1 SNMPv1 passwd1 noAuthPriv -
```

Defining new users with the User-based Security Model

After you have migrated your existing configuration to the SNMPD.CONF file, you can define User-based Security Model (USM) users to take advantage of the enhanced message security provided with SNMPv3. The same VACM_GROUP group names and VACM_VIEWS can be used both for community-based security

and User-based Security. For details on defining USM users, refer to the *z/OS Communications Server: IP Configuration Reference*.

Steps for migrating the osnmp command configuration

The osnmp command configuration does not require any new entries to use community-based security. If you define USM entries in the SNMPD.CONF file, however, you need to define new entries in the OSNMP.CONF file for each USM_USER.

For details about osnmp command configuration and search orders, refer to the *z/OS Communications Server: IP Configuration Reference*.

Appendix B. Related protocol specifications (RFCs)

This appendix lists the related protocol specifications 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.

These documents can be obtained from:

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

You can see Internet drafts at <http://www.ietf.org/ID.html>. See "Draft RFCs" on page 276 for draft RFCs implemented in z/OS V1R4 Communications Server.

You can also request RFCs through electronic mail, from the automated NIC mail server, by sending a message to service@nic.ddn.mil with a subject line of RFC *nnnn* for text versions or a subject line of RFC *nnnn*.PS for PostScript versions. To request a copy of the RFC index, send a message with a subject line of RFC INDEX.

For more information, contact nic@nic.ddn.mil.

Many RFCs are available online. Hard copies of all RFCs are available from the NIC, either individually or by subscription. Online copies are available using FTP from the NIC at the following Web address: <http://www.rfc-editor.org/rfc.html>.

Use FTP to download the files, using the following format:

```
RFC:RFC-INDEX.TXT  
RFC:RFCnnnn.TXT  
RFC:RFCnnnn.PS
```

where:

nnnn Is the RFC number.
TXT Is the text format.
PS Is the PostScript format.

Many features of TCP/IP Services are based on the following RFCs:

RFC	Title and Author
768	<i>User Datagram Protocol</i> J.B. Postel
791	<i>Internet Protocol</i> J.B. Postel
792	<i>Internet Control Message Protocol</i> J.B. Postel
793	<i>Transmission Control Protocol</i> J.B. Postel
821	<i>Simple Mail Transfer Protocol</i> J.B. Postel

- 822 *Standard for the Format of ARPA Internet Text Messages* D. Crocker
- 823 *DARPA Internet Gateway* R.M. Hinden, A. Sheltzer
- 826 *Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.Bit Ethernet Address for Transmission on Ethernet Hardware* D.C. Plummer
- 854 *Telnet Protocol Specification* J.B. Postel, J.K. Reynolds
- 855 *Telnet Option Specification* J.B. Postel, J.K. Reynolds
- 856 *Telnet Binary Transmission* J.B. Postel, J.K. Reynolds
- 857 *Telnet Echo Option* J.B. Postel, J.K. Reynolds
- 858 *Telnet Suppress Go Ahead Option* J.B. Postel, J.K. Reynolds
- 859 *Telnet Status Option* J.B. Postel, J.K. Reynolds
- 860 *Telnet Timing Mark Option* J.B. Postel, J.K. Reynolds
- 861 *Telnet Extended Options—List Option* J.B. Postel, J.K. Reynolds
- 862 *Echo Protocol* J.B. Postel
- 863 *Discard Protocol* J.B. Postel
- 864 *Character Generator Protocol* J.B. Postel
- 877 *Standard for the Transmission of IP Datagrams over Public Data Networks* J.T. Korb
- 885 *Telnet End of Record Option* J.B. Postel
- 896 *Congestion Control in IP/TCP Internetworks* J. Nagle
- 903 *Reverse Address Resolution Protocol* R. Finlayson, T. Mann, J.C. Mogul, M. Theimer
- 904 *Exterior Gateway Protocol Formal Specification* D.L. Mills
- 919 *Broadcasting Internet Datagrams* J.C. Mogul
- 922 *Broadcasting Internet Datagrams in the Presence of Subnets* J.C. Mogul
- 950 *Internet Standard Subnetting Procedure* J.C. Mogul, J.B. Postel
- 952 *DoD Internet Host Table Specification* K. Harrenstien, M.K. Stahl, E.J. Feinler
- 959 *File Transfer Protocol* J.B. Postel, J.K. Reynolds
- 974 *Mail Routing and the Domain Name System* C. Partridge
- 1006 *ISO Transport Service on top of the TCP Version 3* M.T.Rose, D.E. Cass
- 1009 *Requirements for Internet Gateways* R.T. Braden, J.B. Postel
- 1011 *Official Internet Protocols* J. Reynolds, J. Postel
- 1013 *X Window System Protocol, Version 11: Alpha Update* R.W. Scheifler
- 1014 *XDR: External Data Representation Standard* Sun Microsystems Incorporated
- 1027 *Using ARP to Implement Transparent Subnet Gateways* S. Carl-Mitchell, J.S. Quarterman
- 1032 *Domain Administrators Guide* M.K. Stahl
- 1033 *Domain Administrators Operations Guide* M. Lottor

- 1034 *Domain Names—Concepts and Facilities* P.V. Mockapetris
- 1035 *Domain Names—Implementation and Specification* P.V. Mockapetris
- 1042 *Standard for the Transmission of IP Datagrams over IEEE 802 Networks*
J.B. Postel, J.K. Reynolds
- 1044 *Internet Protocol on Network System's HYPERchannel: Protocol
Specification* K. Hardwick, J. Lekashman
- 1055 *Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP* J.L.
Romkey
- 1057 *RPC: Remote Procedure Call Protocol Version 2 Specification* Sun
Microsystems Incorporated
- 1058 *Routing Information Protocol* C.L. Hedrick
- 1060 *Assigned Numbers* J. Reynolds, J. Postel
- 1073 *Telnet Window Size Option* D. Waitzman
- 1079 *Telnet Terminal Speed Option* C.L. Hedrick
- 1091 *Telnet Terminal-Type Option* J. VanBokkelen
- 1094 *NFS: Network File System Protocol Specification* Sun Microsystems
Incorporated
- 1096 *Telnet X Display Location Option* G. Marcy
- 1101 *DNS encoding of network names and other types* P.V. Mockapetris
- 1112 *Host Extensions for IP Multicasting* S. Deering
- 1118 *Hitchhikers Guide to the Internet* E. Krol
- 1122 *Requirements for Internet Hosts—Communication Layers* R.T. Braden
- 1123 *Requirements for Internet Hosts—Application and Support* R.T. Braden
- 1155 *Structure and Identification of Management Information for TCP/IP-Based
Internets* M.T. Rose, K. McCloghrie
- 1156 *Management Information Base for Network Management of TCP/IP-Based
Internets* K. McCloghrie, M.T. Rose
- 1157 *Simple Network Management Protocol (SNMP)* J.D. Case, M. Fedor, M.L.
Schoffstall, C. Davin
- 1158 *Management Information Base for Network Management of TCP/IP-based
internets: MIB-II* M.T. Rose
- 1179 *Line Printer Daemon Protocol* The Wollongong Group, L. McLaughlin III
- 1180 *TCP/IP Tutorial* T.J. Socolofsky, C.J. Kale
- 1183 *New DNS RR Definitions* C.F. Everhart, L.A. Mamakos, R. Ullmann, P.V.
Mockapetris, (Updates RFC 1034, RFC 1035)
- 1184 *Telnet Linemode Option* D. Borman
- 1187 *Bulk Table Retrieval with the SNMP* M.T. Rose, K. McCloghrie, J.R. Davin
- 1188 *Proposed Standard for the Transmission of IP Datagrams over FDDI
Networks* D. Katz
- 1191 *Path MTU Discovery* J. Mogul, S. Deering
- 1198 *FYI on the X Window System* R.W. Scheifler

- 1207 *FYI on Questions and Answers: Answers to Commonly Asked "Experienced Internet User" Questions* G.S. Malkin, A.N. Marine, J.K. Reynolds
- 1208 *Glossary of Networking Terms* O.J. Jacobsen, D.C. Lynch
- 1213 *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II* K. McCloghrie, M.T. Rose
- 1215 *Convention for Defining Traps for Use with the SNMP* M.T. Rose
- 1228 *SNMP-DPI Simple Network Management Protocol Distributed Program Interface* G.C. Carpenter, B. Wijnen
- 1229 *Extensions to the Generic-Interface MIB* K. McCloghrie
- 1230 *IEEE 802.4 Token Bus MIB* K. McCloghrie, R. Fox
- 1231 *IEEE 802.5 Token Ring MIB* K. McCloghrie, R. Fox, E. Decker
- 1236 *IP to X.121 Address Mapping for DDN* L. Morales, P. Hasse
- 1267 *A Border Gateway Protocol 3 (BGP-3)* K. Lougheed, Y. Rekhter
- 1268 *Application of the Border Gateway Protocol in the Internet* Y. Rekhter, P. Gross
- 1269 *Definitions of Managed Objects for the Border Gateway Protocol (Version 3)* S. Willis, J. Burruss
- 1270 *SNMP Communications Services* F. Kastenholz, ed.
- 1321 *The MD5 Message-Digest Algorithm* R. Rivest
- 1323 *TCP Extensions for High Performance* V. Jacobson, R. Braden, D. Borman
- 1325 *FYI on Questions and Answers: Answers to Commonly Asked "New Internet User" Questions* G.S. Malkin, A.N. Marine
- 1340 *Assigned Numbers* J.K. Reynolds, J.B. Postel
- 1348 *DNS NSAP RRs* B. Manning
- 1349 *Type of Service in the Internet Protocol Suite* P. Almquist
- 1350 *TFTP Protocol* K.R. Sollins
- 1351 *SNMP Administrative Model* J. Davin, J. Galvin, K. McCloghrie
- 1352 *SNMP Security Protocols* J. Galvin, K. McCloghrie, J. Davin
- 1353 *Definitions of Managed Objects for Administration of SNMP Parties* K. McCloghrie, J. Davin, J. Galvin
- 1354 *IP Forwarding Table MIB* F. Baker
- 1356 *Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode* A. Malis, D. Robinson, R. Ullmann
- 1363 *A Proposed Flow Specification* C. Partridge
- 1372 *Telnet Remote Flow Control Option* D. Borman, C. L. Hedrick
- 1374 *IP and ARP on HIPPI* J. Renwick, A. Nicholson
- 1381 *SNMP MIB Extension for X.25 LAPB* D. Throop, F. Baker
- 1382 *SNMP MIB Extension for the X.25 Packet Layer* D. Throop
- 1387 *RIP Version 2 Protocol Analysis* G. Malkin
- 1388 *RIP Version 2—Carrying Additional Information* G. Malkin

- 1389 *RIP Version 2 MIB Extension* G. Malkin
- 1390 *Transmission of IP and ARP over FDDI Networks* D. Katz
- 1393 *Traceroute Using an IP Option* G. Malkin
- 1397 *Default Route Advertisement In BGP2 And BGP3 Versions of the Border Gateway Protocol* D. Haskin
- 1398 *Definitions of Managed Objects for the Ethernet-Like Interface Types* F. Kastenholz
- 1416 *Telnet Authentication Option* D. Borman, ed.
- 1464 *Using the Domain Name System to Store Arbitrary String Attributes* R. Rosenbaum
- 1469 *IP Multicast over Token-Ring Local Area Networks* T. Pusateri
- 1535 *A Security Problem and Proposed Correction With Widely Deployed DNS Software* E. Gavron
- 1536 *Common DNS Implementation Errors and Suggested Fixes* A. Kumar, J. Postel, C. Neuman, P. Danzig, S. Miller
- 1537 *Common DNS Data File Configuration Errors* P. Beertema
- 1540 *IAB Official Protocol Standards* J.B. Postel
- 1571 *Telnet Environment Option Interoperability Issues* D. Borman
- 1572 *Telnet Environment Option* S. Alexander
- 1577 *Classical IP and ARP over ATM* M. Laubach
- 1583 *OSPF Version 2* J. Moy
- 1591 *Domain Name System Structure and Delegation* J. Postel
- 1592 *Simple Network Management Protocol Distributed Protocol Interface Version 2.0* B. Wijnen, G. Carpenter, K. Curran, A. Sehgal, G. Waters
- 1594 *FYI on Questions and Answers: Answers to Commonly Asked "New Internet User" Questions* A.N. Marine, J. Reynolds, G.S. Malkin
- 1695 *Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2* M. Ahmed, K. Tesink
- 1706 *DNS NSAP Resource Records* B. Manning, R. Colella
- 1713 *Tools for DNS debugging* A. Romao
- 1723 *RIP Version 2—Carrying Additional Information* G. Malkin
- 1766 *Tags for the Identification of Languages* H. Alvestrand
- 1794 *DNS Support for Load Balancing* T. Brisco
- 1832 *XDR: External Data Representation Standard* R. Srinivasan
- 1850 *OSPF Version 2 Management Information Base* F. Baker, R. Coltun
- 1876 *A Means for Expressing Location Information in the Domain Name System* C. Davis, P. Vixie, T. Goodwin, I. Dickinson
- 1886 *DNS Extensions to support IP version 6* S. Thomson, C. Huitema
- 1901 *Introduction to Community-Based SNMPv2* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

- 1902** *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser
- 1903** *Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser
- 1904** *Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser
- 1905** *Protocols Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser
- 1906** *Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser
- 1907** *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser
- 1908** *Coexistence between Version 1 and Version 2 of the Internet-Standard Network Management Framework* J. Case, K. McCloghrie, M. Rose, S. Waldbusser
- 1912** *Common DNS Operational and Configuration Errors* D. Barr
- 1918** *Address Allocation for Private Internets* Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear
- 1928** *SOCKS Protocol Version 5* M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones
- 1939** *Post Office Protocol-Version 3* J. Myers, M. Rose
- 1981** *Path MTU Discovery for IP version 6* J. McCann, S. Deering, J. Mogul
- 1982** *Serial Number Arithmetic* R. Elz, R. Bush
- 1995** *Incremental Zone Transfer in DNS* M. Ohta
- 1996** *A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)* P. Vixie
- 2010** *Operational Criteria for Root Name Servers* B. Manning, P. Vixie
- 2011** *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2* K. McCloghrie
- 2012** *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2* K. McCloghrie
- 2013** *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2* K. McCloghrie
- 2052** *A DNS RR for specifying the location of services (DNS SRV)* A. Gulbrandsen, P. Vixie
- 2065** *Domain Name System Security Extensions* D. Eastlake, C. Kaufman
- 2096** *IP Forwarding Table MIB* F. Baker
- 2104** *HMAC: Keyed-Hashing for Message Authentication* H. Krawczyk, M. Bellare, R. Canetti
- 2132** *DHCP Options and BOOTP Vendor Extensions* S. Alexander, R. Droms
- 2133** *Basic Socket Interface Extensions for IPv6* R. Gilligan, S. Thomson, J. Bound, W. Stevens

- 2137 *Secure Domain Name System Dynamic Update* D. Eastlake
- 2163 *Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)* C. Allocchio
- 2168 *Resolution of Uniform Resource Identifiers using the Domain Name System* R. Daniel, M. Mealling
- 2178 *OSPF Version 2* J. Moy
- 2181 *Clarifications to the DNS Specification* R. Elz, R. Bush
- 2205 *Resource ReSerVation Protocol (RSVP) Version 1* R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin
- 2210 *The Use of RSVP with IETF Integrated Services* J. Wroclawski
- 2211 *Specification of the Controlled-Load Network Element Service* J. Wroclawski
- 2212 *Specification of Guaranteed Quality of Service* S. Shenker, C. Partridge, R. Guerin
- 2215 *General Characterization Parameters for Integrated Service Network Elements* S. Shenker, J. Wroclawski
- 2219 *Use of DNS Aliases for Network Services* M. Hamilton, R. Wright
- 2228 *FTP Security Extensions* M. Horowitz, S. Lunt
- 2230 *Key Exchange Delegation Record for the DNS* R. Atkinson
- 2233 *The Interfaces Group MIB Using SMIv2* K. McCloghrie, F. Kastenholz
- 2240 *A Legal Basis for Domain Name Allocation* O. Vaughn
- 2246 *The TLS Protocol Version 1.0* T. Dierks, C. Allen
- 2308 *Negative Caching of DNS Queries (DNS NCACHE)* M. Andrews
- 2317 *Classless IN-ADDR.ARPA delegation* H. Eidnes, G. de Groot, P. Vixie
- 2320 *Definitions of Managed Objects for Classical IP and ARP over ATM Using SMIv2* M. Greene, J. Luciani, K. White, T. Kuo
- 2328 *OSPF Version 2* J. Moy
- 2345 *Domain Names and Company Name Retrieval* J. Klensin, T. Wolf, G. Oglesby
- 2352 *A Convention for Using Legal Names as Domain Names* O. Vaughn
- 2355 *TN3270 Enhancements* B. Kelly
- 2373 *IP Version 6 Addressing Architecture* R. Hinden, M. O'Dell, S. Deering
- 2374 *An IPv6 Aggregatable Global Unicast Address Format* R. Hinden, M. O'Dell, S. Deering
- 2375 *IPv6 Multicast Address Assignments* R. Hinden, S. Deering
- 2389 *Feature negotiation mechanism for the File Transfer Protocol* P. Hethmon, R. Elz
- 2428 *FTP Extensions for IPv6 and NATs* M. Allman, S. Ostermann, C. Metz
- 2460 *Internet Protocol, Version 6 (IPv6) Specification* S. Deering, R. Hinden
- 2461 *Neighbor Discovery for IP Version 6 (IPv6)* T. Narten, E. Nordmark, W. Simpson
- 2462 *IPv6 Stateless Address Autoconfiguration* S. Thomson, T. Narten

- | **2464** *Transmission of IPv6 Packets over Ethernet Networks* M. Crawford
- | **2474** *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* K. Nichols, S. Blake, F. Baker, D. Black
- | **2535** *Domain Name System Security Extensions* D. Eastlake
- | **2539** *Storage of Diffie-Hellman Keys in the Domain Name System (DNS)* D. Eastlake
- | **2553** *Basic Socket Interface Extensions for IPv6* R. Gilligan, S. Thomson, J. Bound, W. Stevens
- | **2571** *An Architecture for Describing SNMP Management Frameworks* D. Harrington, R. Presuhn, B. Wijnen
- | **2572** *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* J. Case, D. Harrington, R. Presuhn, B. Wijnen
- | **2573** *SNMP Applications* D. Levi, P. Meyer, B. Stewart
- | **2574** *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* U. Blumenthal, B. Wijnen
- | **2575** *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* B. Wijnen, R. Presuhn, K. McCloghrie
- | **2578** *Structure of Management Information Version 2 (SMIv2)* K. McCloghrie, D. Perkins, J. Schoenwaelder
- | **2640** *Internationalization of the File Transfer Protocol* B. Curtin
- | **2665** *Definitions of Managed Objects for the Ethernet-like Interface Types* J. Flick, J. Johnson
- | **2672** *Non-Terminal DNS Name Redirection* M. Crawford
- | **2710** *Multicast Listener Discovery (MLD) for IPv6* S. Deering, W. Fenner, B. Haberman
- | **2711** *IPv6 Router Alert Option* C. Partridge, A. Jackson
- | **2758** *Definitions of Managed Objects for Service Level Agreements Performance Monitoring* K. White
- | **2845** *Secret Key Transaction Authentication for DNS (TSIG)* P. Vixie, O. Gudmundsson, D. Eastlake, B. Wellington
- | **2874** *DNS Extensions to Support IPv6 Address Aggregation and Renumbering* M. Crawford, C. Huitema
- | **2941** *Telnet Authentication Option* T. Ts'o, ed., J. Altman
- | **2942** *Telnet Authentication: Kerberos Version 5* T. Ts'o
- | **2946** *Telnet Data Encryption Option* T. Ts'o
- | **2952** *Telnet Encryption: DES 64 bit Cipher Feedback* T. Ts'o
- | **2953** *Telnet Encryption: DES 64 bit Output Feedback* T. Ts'o, ed.
- | **3060** *Policy Core Information Model—Version 1 Specification* B. Moore, E. Ellesson, J. Strassner, A. Westerinen

Draft RFCs

Several areas of IPv6 implementation include elements of the following draft RFCs and are subject to change during the RFC review process.

| **Advanced Sockets API for IPv6**

| W. Richard Stevens, Matt Thomas, Erik Nordmark, Tatuya Jinmei

| **Basic Socket Interface Extensions for IPv6**

| R.E. Gilligan, S. Thomson, J. Bound, J. McCann, W. R. Stevens

| **Default Address Selection for IPv6**

| R. Draves

| **Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version
6 (IPv6) Specification**

| A. Conta, S. Deering

| **IP Version 6 Addressing Architecture**

| R. Hinden, S. Deering

Appendix C. Information APARs

This appendix lists information APARs for IP and SNA documents.

Notes:

1. Information APARs contain updates to previous editions of the manuals listed below. Documents updated for V1R4 are complete except for the updates contained in the information APARs that may be issued after V1R4 documents went to press.
2. Information APARs are predefined for z/OS V1R4 Communications Server and may not contain updates.
3. Information APARs for OS/390 documents are in the document called *OS/390 DOC APAR and PTF ++HOLD Documentation*, which can be found at http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/IDDOCMST/CCONTENTS.
4. Information APARs for z/OS documents are in the document called *z/OS and z/OS.e DOC APAR and PTF ++HOLD Documentation*, which can be found at http://publibz.boulder.ibm.com:80/cgi-bin/bookmgr_OS390/BOOKS/ZIDOCMST/CCONTENTS.

Information APARs for IP documents

Table 193 lists information APARs for IP documents.

Table 193. IP information APARs

Title	z/OS CS V1R4	z/OS CS V1R2	CS for OS/390 2.10 and z/OS CS V1R1	CS for OS/390 2.8
IP API Guide	ii13255	ii12861	ii12371	ii11635
IP CICS Sockets Guide	ii13257	ii12862		ii11626
IP Configuration				ii11620 ii12068 ii12353 ii12649 ii13018
IP Configuration Guide	ii13244	ii12498 ii13087	ii12362 ii12493 ii13006	
IP Configuration Reference	ii13245	ii12499	ii12363 ii12494 ii12712	
IP Diagnosis	ii13249	ii12503	ii12366 ii12495	ii11628
IP Messages Volume 1	ii13250	ii12857 ii13229	ii12367	ii11630 13230
IP Messages Volume 2	ii13251	ii12858	ii12368	ii11631
IP Messages Volume 3	ii13252	ii12859	ii12369 12990	ii11632 ii12883
IP Messages Volume 4	ii13253	ii12860		
IP Migration	ii13242	ii12497	ii12361	ii11618

Table 193. IP information APARs (continued)

Title	z/OS CS V1R4	z/OS CS V1R2	CS for OS/390 2.10 and z/OS CS V1R1	CS for OS/390 2.8
IP Network and Application Design Guide	ii13243			
IP Network Print Facility		ii12864		ii11627
IP Programmer's Reference	ii13256	ii12505		ii11634
IP and SNA Codes	ii13254	ii12504	ii12370	ii11917
IP User's Guide			ii12365 ii13060	ii11625
IP User's Guide and Commands	ii13247	ii12501	ii12365 ii13060	ii11625
IP System Admin Guide	ii13248	ii12502		
Quick Reference	ii13246	ii12500	ii12364	

Information APARs for SNA documents

Table 194 lists information APARs for SNA documents.

Table 194. SNA information APARs

Title	z/OS CS V1R4	z/OS CS V1R2	CS for OS/390 2.10 and z/OS CS V1R1	CS for OS/390 2.8
Anynet SNA over TCP/IP				ii11922
Anynet Sockets over SNA				ii11921
CSM Guide				
IP and SNA Codes	ii13254	ii12504	ii12370	ii11917
SNA Customization	ii13240	ii12872	ii12388	ii11923
SNA Diagnosis	ii13236	ii12490 ii13034	ii12389	ii11915
SNA Messages	ii13238	ii12491	ii12382 ii12383	ii11916
SNA Network Implementation Guide	ii13234	ii12487	ii12381	ii11911
SNA Operation	ii13237	ii12489	ii12384	ii11914
SNA Migration	ii13233	ii12486	ii12386	ii11910
SNA Programming	ii13241	ii13033	ii12385	ii11920
Quick Reference	ii13246	ii12500	ii12364	ii11913
SNA Resource Definition Reference	ii13235	ii12488	ii12380 ii12567	ii11912 ii12568
SNA Resource Definition Samples				
SNA Data Areas	ii13239	ii12492	ii12387	ii11617

Other information APARs

Table 195 on page 281 lists information APARs not related to documents.

Table 195. Non-document information APARs

Content	Number
OMPROUTE	ii12026
iQDIO	ii11220
index of recommended maintenace for VTAM	ii11220
CSM for VTAM	ii12657
CSM for TCP/IP	ii12658
AHHC, MPC, and CTC	ii01501
DLUR/DLUS for z/OS V1R2	ii12986
Enterprise Extender	ii12223
Generic resources	ii10986
HPR	ii10953
MNPS	ii10370
Performance	ii11710 ii11711 ii11712

Appendix D. Accessibility

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 it to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Volume 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.

Notices

IBM may not offer all of the products, services, or features discussed in this document. 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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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:

Site Counsel
IBM Corporation
P.O.Box 12195
3039 Cornwallis Road
Research Triangle Park, North Carolina 27709-2195
U.S.A

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 information 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.

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 measurement 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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 illustrates 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. 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 IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

This product includes cryptographic software written by Eric Young.

If you are viewing this information softcopy, photographs and color illustrations may not appear.

You can obtain softcopy from the z/OS Collection (SK3T-4269), which contains BookManager and PDF formats of unlicensed books and the z/OS Licensed Product Library (LK3T-4307), which contains BookManager and PDF formats of licensed books.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

ACF/VTAM	Micro Channel
Advanced Peer-to-Peer Networking	MVS
AFP	MVS/DFP
AD/Cycle	MVS/ESA
AIX	MVS/SP
AIX/ESA	MVS/XA
AnyNet	MQ
APL2	Natural
AS/400	NetView
AT	Network Station
BookManager	Nways
BookMaster	Notes
CBPDO	NTune
C/370	NTuneNCP
CICS	OfficeVision/MVS
CICS/ESA	OfficeVision/VM
C/MVS	Open Class
Common User Access	OpenEdition
C Set ++	OS/2
CT	OS/390
CUA	OS/400
DATABASE 2	Parallel Sysplex
DatagLANce	Personal System/2
DB2	PR/SM
DFSMS	PROFS
DFSMSdfp	PS/2
DFSMSHsm	RACF
DFSMS/MVS	Resource Link
DPI	Resource Measurement Facility
Domino	RETAIN
DRDA	RFM
eNetwork	RISC System/6000
Enterprise Systems Architecture/370	RMF
ESA/390	RS/6000
ESCON	S/370
eServer	S/390
ES/3090	SAA
ES/9000	SecureWay
ES/9370	Slate
EtherStreamer	SP
Extended Services	SP2
FAA	SQL/DS
	System/360

FFST	System/370
FFST/2	System/390
FFST/MVS	SystemView
First Failure Support Technology	Tivoli
GDDM	TURBOWAYS
Hardware Configuration Definition	UNIX System Services
IBM	Virtual Machine/Extended Architecture
IBMLink	VM/ESA
IBMLINK	VM/XA
IMS	VSE/ESA
IMS/ESA	VTAM
InfoPrint	WebSphere
Language Environment	XT
LANStreamer	z/Architecture
Library Reader	z/OS
LPDA	z/OS.e
MCS	zSeries
	400
	3090
	3890

Lotus, Freelance, and Word Pro are trademarks of Lotus Development Corporation in the United States, or other countries, or both.

Tivoli and NetView are trademarks of Tivoli Systems Inc. in the United States, or other countries, or both.

DB2 and NetView are registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the U.S., other countries, or both.

The following terms are trademarks of other companies:

ATM is a trademark of Adobe Systems, Incorporated.

BSC is a trademark of BusiSoft Corporation.

CSA is a trademark of Canadian Standards Association.

DCE is a trademark of The Open Software Foundation.

HYPERchannel is a trademark of Network Systems Corporation.

UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through X/Open Company Limited.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both. For a complete list of Intel trademarks, see <http://www.intel.com/sites/corporate/tradmarx.htm> .

Other company, product, and service names may be trademarks or service marks of others.

Index

Special characters

`_BPXK_SETIBMOPT_TRANSPORT` environment variable 58
`hlq.FTP.DATA` data set, FTP client configuration statements 170
`hlq.FTP.DATA` data set, FTP server configuration statements 167

Numerics

2-gigabyte real storage bar 126
3745/46 Channel DLC Devices 163
64-bit real addressing support 126

A

abend trap (Telnet) 217
ACC option 177
Accelerator, HiperSockets 117
access control for FRCA 70
access control, network 69
ACCESSERRORMSG 177
accessibility features 283
activity logging and FTP 176
Adaptive rate-based (ARB) congestion control 142
address, e-mail 193
addressing for OMPROUTE, wildcard IP 105
addressing support, 64-bit real 126
AEZAHLP 65
AF_INET physical file system 5
 common 6
 integrated sockets 6
AF_INET6 79
AF_INET6 network 181
AF_INET6 physical file system 5
AF_INET6 socket addresses 153
AF_UNIX physical file system 5
AHELP 65
algorithm, Nagle 108
Allow Source VIPA 243
ALLOWAPPL 206
ANONYMOUS option in the FTP.DATA server configuration file 183
ANONYMOUS statements 167
anonymous users, password for 193
anonymous, server 194
ANONYMOUSFTPLLOGGING 176
ANONYMOUSFTPLLOGGING statement 167
anonymouslevel keyword 194
API calls, setsockopt and getsockopt 108
API commands, socket 87
API, Callable 159
API, TCP/IP Macro 159
APIs (application programming interfaces) 6
application programming interfaces, types in z/OS
 Communications Server, see also APIs 6
application-driven policy classification 112

ARB 143
ARB congestion control 142
ARP enhancements 146
ASCII support for HFS files FTP 190
Assembler Callable Services, z/OS UNIX, general description 8
ASSORTEDPARMS statement 65, 91
asynchronous transfer mode (ATM), general description 3
ATM (asynchronous transfer mode), general description 3
ATM LE 145
ATMLIS PROFILE.TCPIP configuration statement, updates by release 31
attack detection 95
authentication and FTP 185
AUTHENTICATION_TYPE keyword 107
authentication, network 216
authentication, OSPF MD5 106
authentication, password 107
authorization, RACF for Cache Accelerator 162

B

balancing, workload 118
banners, displaying as reply messages 192
BEGINROUTES / ENDROUTES PROFILE.TCPIP configuration statement, updates by release 31
BEGINROUTES and static routes 104
BEGINVTAM 206
BEGINVTAM / ENDVTAM PROFILE.TCPIP configuration statement, updates by release 31
BIND 4.9.3 mode 261
BIND 9 mode 256
BIND DNS domain data file 250
BIND DNS upgrade 256
BIND-Based DNS name server 249
binding using sever bind control 151
bounce attacks 181
BPXPRMxx 79
BPXPRMxx SYS1.PARMLIB member, updates by release 35

C

C sockets 7
Cache Accelerator 161, 162
Callable API 159
catalog security 182
CCC command 171
CDLC (channel data link control), general description 3
CDLC device driver 163
certificate, X509 V3 221
channel data link control (CDLC), general description 3
Channel DLC Devices, 3745/46 163
channel-to-channel (CTC), general description 3
Chinese standard GB18030 177

CICS (customer information control system) sockets 7
 CICS sockets listener 120
 CINET 192
 CIPHERSUITE statement 168, 170
 Cisco, communicating with 164
 CLAW (common link access to workstation), general
 description 3
 CLAW packing 125, 164
 CLEAR command 171
 Client Identifiers, Telnet 219
 CLIENTAUTH 204
 codepage IBM-5488 177
 command start options, FTP 174
 commands, FTP z/OS UNIX and TSO 171
 commands, IPCS 159
 commands, operator
 See operator commands, updates by release
 commands, socket API 87
 commands, TSO
 See TSO commands, updates by release
 commands, UNIX
 See UNIX commands, updates by release
 common AF_INET
 access by APIs 6
 general description 6
 common link access to workstation (CLAW), general
 description 3
 Communications Server for z/OS, online information xx
 communications storage manager, general description,
 see also CSM 3
 configurable timer, FINWAIT2 130
 configuration files, updates by release 29
 OMPROUTE 29
 Policy Agent 30
 PROFILE.TCPIP 31
 Resolver setup file 30
 SYSLOGD 31
 configuration statements, FTP client 170
 configuration statements, FTP server 167
 connection reset for Sysplex Distributor 114
 connections, Sysplex-wide Dynamic Source VIPAs for
 TCP 66
 CONNTYPE 205
 CONNTYPE NEGTSURE statement 223
 CPROTECT parameter 171
 CRLLDAPSERVER 204
 CSA 124
 CSM (communications storage manager), general
 description 3
 CTC (channel-to-channel), general description 3
 CTIEZB00 SYS1.PARMLIB member, updates by
 release 35
 CTIIDS00 SYS1.PARMLIB member, updates by
 release 35
 CTIRES00 SYS1.PARMLIB member, updates by
 release 35
 CTRACE COMP(SYSTCPDA) IPCS subcommand 61
 CTRACE COMP(SYSTCPIS) IPCS subcommand 62
 CTRACE COMP(SYSTCPRE) IPCS subcommand 62
 CTRACE packet trace formatter 113
 CTRACE, SYSTCPIS 96

customer information control system sockets, general
 description, see also CICS 7
 customizing z/OS using GUI panels 123
 CWD command 187

D

data set allocation and FTP 198
 data sets, distribution library 16
 DCAS 155, 221
 DDname support 201
 DEBUG 204, 205, 213, 217
 DEBUG command 171
 DEBUG statement 168, 170
 DEBUG subcommand 191
 DEBUGONSITE statement 168
 DEFAULTAPPL 206
 DEFAULTLUSSPEC 206
 DEFAULTPRT 207
 DEFAULTPRTSPEC 207
 DEFAULTTCPIPDATA 92
 defining an OMVS segment 94, 95
 DELETE DEVICE PROFILE.TCPIP configuration
 statement, updates by release 31
 DELETE LINK PROFILE.TCPIP configuration statement,
 updates by release 31
 DELETE PORT PROFILE.TCPIP configuration
 statement, updates by release 32
 DEVICE and LINK for MPCIPA devices
 PROFILE.TCPIP configuration statement, updates by
 release 32
 DEVICE for CLAW devices PROFILE.TCPIP
 configuration statement, updates by release 32
 devices, MPCIPA 145
 DEVLINKS/-d report, netstat 146
 diagnosing traces using FTP 191
 diagnosing using TCP/IP tracing 160
 diagnostics, TN3270 217
 Differentiated Services (DS) field 112
 dig 251
 DIG 14
 DIG TSO command, updates by release 43
 Digital Certificate Access Server (DCAS) 155, 221
 DIR command 171
 DIR output 182
 disability, physical 283
 dispatcher routing 135
 DISPLAY TCPIP,,HELP operator command, updates by
 release 36
 DISPLAY TCPIP,,NETSTAT operator command, updates
 by release 36
 DISPLAY TCPIP,,STOR operator command, updates by
 release 41
 DISPLAY TCPIP,,SYSPLEX operator command, updates
 by release 41
 displaying routes 163
 distributed programming interface, general
 description 16
 distribution library data sets 16
 DNS (domain name system) server 249
 DNS BIND 4.9.3 mode 261

- DNS updates for z/OS V1R4 CS 252
- DNS upgrade, BIND 256
- DNS, online information xxi
- dnsdomainname 14
- dnsmigrate 257
- documents, licensed xxi
- DOMAIN TCPIP.DATA statement, updates by
 - release 31
- domainname 14
- DPI (distributed programming interface) 16
- DPI (distributed protocol interface) 233
- DS (Differentiated Services) field 112
- DSNAME parameter 122
- DUMP command 171
- DUMP statement 168, 170
- DUMP subcommand 191
- DUMPSITE statement 168
- Dynamic Source VIPAs for TCP connections,
 - Sysplex-wide 66
- Dynamic VIPA 119
- Dynamic XCF 114

E

- e-mail address 193
- ENCODING statement 167, 170
- ENCRYPTION 204
- encryption features 20
- Enterprise Extender 125
- environment variables for DNS 252
- environment variables, updates by release 58
- ephemeral ports 67
- error messages, turning off exception debug 213
- event trace 72
- EXCEPTION option 213
- EXCEPTSTATS 96
- exit to filter unwanted mail, SMTP 122
- Express Logon 155
- Express Logon Feature using TN3270E Server 221
- EXPRESSLOGON 205
- EXTENSIONS statement 168, 188
- EZAIPCSP SYS1.PARMLIB member, updates by
 - release 35
- EZAZSSI 129
- EZBZSMTP macro 122
- EZZ6317I warning message 236

F

- failure replies, log-in 176
- fast connection reset after system failure 114
- Fast Ethernet for QDIO 145
- fast local sockets 160
- Fast Response Cache Accelerator 161
- FEAT command 171
- FEATURE subcommand 189
- filter unwanted mail, SMTP exit to 122
- filter, INTFName/-K 75
- filtering using Netstat commands 109
- FINWAIT2 configurable timer 130
- firewall 162

- foreign-host start option 172
- format type 118, SMF 121
- format type 119, SMF 122
- formatter, CTRACE packet trace 113
- FRCA 70, 161
- FTCHKCMD user written exit 200
- FTP server and client 167
 - activity logging 176
 - authentication 185
 - batch job comments 201
 - command start options 174
 - Common INET stack 192
 - configuring user-level server options 187
 - CS for OS/390 V2R10 release summary 191
 - DDname support 201
 - extending SMF record 194
 - file transfers that are encoded 177
 - FTP client configuration statements 170
 - FTP server configuration statements 167
 - IPv6 support 180
 - ISPF statistics 186
 - JES interface 199
 - Kerberos support 185
 - load module transfer 196
 - native ASCII support for HFS files 190
 - password failure replies 176
 - requesting e-mail address as a password for
 - anonymous users 193
 - restarting file transfer 187
 - RFC updates 188
 - server anonymous enhancements 194
 - server security 181
 - SITE and LOCSITE allocation keywords 198
 - socksify FTP client 183
 - STAT and LOCSTAT commands 192
 - stream mode restart 187
 - TLS enablement 184
 - trace enhancements 191
 - transferring MVS data sets with FTP URL 198
 - UNIX and TSO commands 171
 - user exits 178, 200
 - using substitution characters 175
 - welcome page support 192
 - z/OS V1R2 CS release summary 181
 - z/OS V1R4 CS release summary 175
- FTP URL, coding 198
- FTP.DATA data set, FTP client configuration
 - statements 170
- FTP.DATA data set, FTP server configuration
 - statements 167
- FTPLOGGING 176
- FTPLOGGING statement 167

G

- GATE/-g 162
- getsockopt and setsocket API calls 108
- GLOBALCONFIG POOLLIMIT statement 125
- GLOBALCONFIG PROFILE.TCPIP configuration
 - statement, updates by release 32
- GLOBALTCPIPDATA 92

GRE tunnels 119
GSSAPI authentication 185
GUI panels, customizing z/OS using 123

H

HELP 65
HFS (hierarchical file system) parts for z/OS
 Communications Server 16, 18
HFS files and native ASCII support for FTP 190
High Speed Access Services 154
HiperSockets 4, 114
HiperSockets Accelerator 117
home address 160
HOME PROFILE.TCPIP configuration statement,
 updates by release 32
HOMETEST TSO command, updates by release 43
host 14
host-name, FTP client subcommand open
 parameter 172
hostname 14
HSAS 154
HSPA 154
HYPERchannel, general description 4

I

I/O process model 3
IBM Software Support Center, contacting xxii
IBM-5488 codepage 177
ICMP (internet control message protocol), general
 description 4
Identifiers, Telnet Client 219
IDS 95
IDS/-k command, Netstat 96
IKE, (Internet Key Exchange) 152
IKJTSOxx SYS1.PARMLIB member, updates by
 release 35
INET, Common 192
INETSTAT IPCS subcommand 62
information APARs for IP-related documents 279
information APARs for non- document information 280
information APARs for SNA-related documents 280
INTERFACE PROFILE.TCPIP configuration statement,
 updates by release 32
Internal Queued Direct I/O, or iQDIO 114
internet control message protocol (ICMP), general
 description 4
Internet Key Exchange (IKE) 152
internet protocol (IP), definition 2
Internet, finding z/OS information online xx
INTFName/-K filter 75
Intrusion Detection Services (IDS) 95
IP (internet protocol), definition 2
IP addressing, wildcard 105
IP message passing 114
IP routing 162
ip_qos_classification_data option 112
IPCONFIG PROFILE.TCPIP configuration statement,
 updates by release 32
IPCONFIG6 80

IPCONFIG6 PROFILE.TCPIP configuration statement,
 updates by release 32
IPCS commands 159
IPCS subcommands, updates by release 61
IPSec enhancements 130
IPSec tunnels 68
IPv6 API 153
IPv6 socket APIs 58
IPv6 support 79
 adding and deleting addresses to INTERFACE
 definition 82
 adding IPv6 route to IP route table 81
 address support 80
 applications 83
 associating jobs 82
 configuration changes 80
 configuring and deleting interfaces 82
 control packet tracing for IPv6 address 81
 deprecating IPv6 address 82
 enable IPv6 forwarding 81
 enable IPv6 Source VIPA support 81
 enable multipath route selection 81
 enabling 79
 event trace enhancements 86
 FTP connectivity 180
 ignore ICMPv6 redirects 81
 ignoring hop limits in Router Advertisement
 messages 82
 IPv6 IPCS subcommands formatting 86
 Netstat 84
 Ping 85
 RAS packet trace and data trace 87
 resolver 82
 set IPv6 hop limit 81
 set IPv6 ICMP error limit 81
 socket API commands 87
 Traceroute 85
 tracing socket data for IPv6 address 81
iQDIO 4
iQDIO (Internal Queued Direct I/O) 114
iQDIO and QDIO storage 78
ISPF statistics 186
ISPFSTATS statement 168, 170

J

JES keywords that allow output selection, FTP 199
JES processing statements 168
job name prefix 153

K

KDC (Key Distribution Center) 111
KEEPALIVEOPTIONS statement 65, 91
KEEPINACTIVE 205
Kerberos support 91
 CS for OS/390 Kerberos support discontinued in
 z/OS CS V1R2 91
 for the FTP server and client 185
 for z/OS UNIX RSHD 111
 for z/OS UNIX Telnet (otelnctd) server 216

Key Distribution Center (KDC) 111
Key Exchange (IKE), Internet 152
key generation commands 233
keyboard 283
KEYRING 204, 205
KEYRING statement 168, 170

L

LAN channel station (LCS), general description 4
LANG command 172
LCS (LAN channel station), general description 4
LDAP enhancements 139
LDAP policy 97, 100
LFS (logical file system), general description 5
license, patent, and copyright information 285
licensed documents xxi
Limit mode 95
Limit mode (TRM) 143
limit mode, simulated 95
line printer daemon (LPD), general description 11
line printer requester (LPR), general description 11
LINEMODEAPPL 207
listener, CICS sockets 120
load balancing (MNLB), multiNode 118
load library 65
load module transfer by using FTP 196
LOCSITE command 172, 198
LOCSTAT command 172, 192
Log mode (TRM) 143
log-in failure replies and FTP 176
logical file system (LFS), general description 5
LOOKUP directive 92
LOOKUP TCPIP.DATA statement, updates by release 31
loopback address 160
LPARs and HiperSockets 114
LPD (line printer daemon), general description 11
LPR (line printer requester), general description 11
LU mapping 214
LU name lookup, sequential 215
LUGROUP 207
LUMAP 207

M

Macro API, TCP/IP 159
mail, SMTP exit to filter 122
Managed System Infrastructure for Setup (msys for Setup) 71, 123
management information base (MIB), general description 231
mapping Objects to clients 219
mapping user priorities 112
MBDATACONN statement 167, 170
MD5 authentication, OSPF 106
MDEL command 172
MDTM command 197
Message Digest (MD5) authentication, OSPF 106
message passing, IP 114
MGET command 172

MIB (management information base), general description 231
MIB objects, setting 236
middle tier TN3270 servers 155
migrating OROUTED to OMPROUTE 102
migration checklist 27
MISCSERV server, general description 15
MNLB (MultiNode Load Balancing) 118
MODIFY command 173, 191
MODIFY PAGENT_procname operator command, updates by release 41
MODIFY remote_execution_server_procname operator command, updates by release 41
MODIFY RESOLVER_procname operator command, updates by release 41
MODIFY RESOLVER,REFRESH command 92
MPC (multipath channel) 3
MPCIPA 143
MPCIPA device 117
MPCIPA devices 145, 146
MPCOSA 4
MPCPTP (multi-path channel point-to-point) general description 4
MPUT command 172
msys for Setup 71, 123
MTU traffic and CLAW performance 164
multi-path channel point-to-point, general description, see also MPCPTP 4
MultiNode Load Balancing (MNLB) 118
multipath channel, general description, see also MPC 3
MVS (multiple virtual storage), general description 1
MVS data sets 16
MVS data sets with FTP URL 198
MVS load modules, transferring by using FTP 196
MVSURLKEY statement 169

N

Nagle algorithm 108
name lookup, sequential LU 215
name server, dynamic domain name system 249
named 251
NAMESERVER TCPIP.DATA statement, updates by release 31
native ASCII support for HFS files, FTP 190
native socket API TCP_NODELAY support 108
NCPROUTE, general description 12
NCS (network computing system), general description 15
NDB (network database), general description 15
Neighbor Discovery 86
NETACCESS/ENDNETACCESS PROFILE.TCPIP configuration statement, updates by release 33
Netstat 74
netstat DEVLINKS/-d report 146
Netstat filter enhancements for z/OS V1R2 109
Netstat GATE/-g 162
Netstat IDS/-k command 96
Netstat performance commands for z/OS V1R2 109
netstat route 163

Netstat ROUTE/-r 162
NETSTAT TSO command, updates by release 43
NETSTAT, general description 10
network access control 69
network access, user control 151
network authentication 216
network computing system (NCS), general description 15
network database (NDB), general description 15
network print facility, general description, see also NPF 12
NETWORK statement 79
non-disruptive VIPA takeover 138
NPF (network print facility) 12
nslookup 251, 252
nslookup, general description 14
nsupdate 14, 251

O

Objects to clients, mapping 219
objects, setting MIB 236
OMPROUTE 102
 allowing RIP1 and RIP2 packets over the same interface 103
 OSPF MD5 authentication 106
 replacing static routes 104
 RIP filter for ignoring routing table broadcasts 106
 wildcard IP addressing 105
OMPROUTE configuration file, updates by release 29
OMPROUTE SNMP subagent, general description 10
OMPROUTE subagent
 general description 233
OMPROUTE_DEBUG_FILE_CONTROL environment variable 58
OMVS segment, defining 94, 95
On-Demand Tunnels 152
ONC/RPC (open network computing/remote procedure call) programming libraries 15
onetstat UNIX command, updates by release 50
onslookup 251
Open Network Computing/Remote Procedure Call programming libraries, general description, see also ONC/RPC 15
Open Shortest Path First (OSPF) MD5 authentication 106
operator commands, Telnet 209
operator commands, updates by release 36
 DISPLAY TCPIP,,HELP 36
 DISPLAY TCPIP,,NETSTAT 36
 DISPLAY TCPIP,,STOR 41
 DISPLAY TCPIP,,SYSPLEX 41
 MODIFY PAGENT_procname 41
 MODIFY remote_execution_server_procname 41
 MODIFY RESOLVER_procname 41
 TRACE CT,ON,COMP= SYSTCPIP 42
 TRACE CT,ON,COMP= SYSTCPIS 42
 TRACE CT,ON,COMP= SYSTCPRE,SUB=(resolverprocname) 42
 VARY TCPIP,,DATTRACE 42
 VARY TCPIP,,PKTTRACE 42
operator commands, updates by release (*continued*)
 VARY TCPIP,,PURGECache 42
oping UNIX command, updates by release 56
OPTIONS directive 92
OPTIONS TCPIP.DATA statement, updates by release 31
options, FTP command start 174
OPTS command 173
OROUTED to OMPROUTE migration 102
orouted UNIX command, updates by release 56
orshd UNIX command, updates by release 56
OSA SNMP subagent support 72
OSA-Express 145
OSA-Express QDIO connection 117
OSA-Express token ring support 127
OSF (Open Software Foundation)/Motif programming library 15
osnmp 267
 general description 232
osnmpd 265
OSNMPD.DATA file 236
OSPF MD5 authentication 106
otelnetd 209, 216, 222
otracer UNIX command, updates by release 56

P

packet internet groper (PING), general description 10
packet size, estimating 164
packet trace 87
packet trace formatter, CTRACE 113
packets of data, transmitting 152
packets, RIP1 and RIP2 103
packets, source and destination management 160
packing, CLAW 125, 164
pagent UNIX command, updates by release 57
PAGENT_LOG_FILE_CONTROL environment variable 58
parameters, Telnet 204
PARMSGROUP statement 223
PARMSGROUP statement block 208
PARMSMAP 208
PARMSMAP statement 223
Pascal sockets
 general description 6
pasearch command 10, 139
pasearch UNIX command, updates by release 57
PASS command failure 176
password authentication 107
password for anonymous users 193
password, surrogate 183
Path MTU Discovery 130
performance, CLAW packing 164
PFS (physical file system) 5
physical file system, general description, see also PFS 5
Ping 75
PING (packet internet groper), general description 10
PING TSO command, updates by release 48
ping UNIX command, updates by release 57

PKTTRACE PROFILE.TCPIP configuration statement, updates by release 33

Policy Agent configuration file, updates by release 30

policy agent enhancements 139

Policy Agent enhancements in z/OS V1R2 100

Policy agent, general description 10

policy agent, QoS enforcement 142

policy classification, application-driven 112

policy enhancements, Sysplex Distributor 98

policy management 95

policy schema 100

Port Access Control 148

PORT commands, rejecting 182

port connections, limiting using TRM 142

PORT PROFILE.TCPIP configuration statement, updates by release 33

port qualification, Telnet 211

PORTCOMMAND statements 169

portmapper 14

PORTRANGE PROFILE.TCPIP configuration statement, updates by release 33

ports, ephemeral 67

POSIX standard

- application behavior in z/OS Communications Server 5
- using z/OS UNIX C sockets API with 8

prefix, job name 153

printer specification, Telnet 212

priority tagging, virtual LAN 112

PRIROUTER 117

PRIVATE command 173

PRIVATE statement 170

PROFILE.TCPIP configuration statements 203, 204, 205, 206

PROFILE.TCPIP configuration statements and parameters, updates by release 31

- ATMLIS 31
- BEGINROUTES / ENDROUTES 31
- BEGINVTAM / ENDVTAM 31
- DELETE DEVICE 31
- DELETE LINK 31
- DELETE PORT 32
- DEVICE and LINK for MPCIPA devices 32
- DEVICE for CLAW devices 32
- GLOBALCONFIG 32
- HOME statement 32
- INTERFACE statement 32
- IPCONFIG statement 32
- IPCONFIG6 statement 32
- LINK statement 32
- NETACCESS/ENDNETACCESS statement 33
- PKTTRACE statement 33
- PORT statement 33
- PORTRANGE statement 33
- ROUTE statement 33
- SACONFIG statement 34
- SMFCONFIG statement 34
- TCPCONFIG statement 34
- VIPABACKUP statement 34
- VIPADefINE statement 34
- VIPADISTRIBUTE statement 34

PROFILE.TCPIP configuration statements and parameters, updates by release (*continued*)

- VIPARANGE statement 34
- VIPASMPARMS statement 34

PROGxx SYS1.PARMLIB member, updates by release 35

PROTECT parameter 170, 173

protocol suite, z/OS Communications Server TCP/IP 2

PRTGROUP 208

PRTMAP 208

PTRDEFAULTAPPL 208

PW.SRC file 265

pwtokey command 107

Q

QDIO and iQDIO storage 78

QDIO connection, OSA-Express 117

QDIO Queue Management 144

QDIO, Fast Ethernet 145

QINIT option 214

QoS fractions 98

QoS service levels 112

Quality of Service (QoS) Enhancements, Service Level Policy 141

Quality of Service user priorities, mapping 112

queue management 144

R

RACF (resource access control facility) 162

RACF support, surrogate 183

Random Early Slowdown (RES) 144

RAPI (RSVP API) 16

RAW protocol, general description 5

real addressing support, 64-bit 126

RECEIVE_RIP 104

remote execution protocol daemon, general description, see also REXECD 12

remote execution protocol, general description, see also REXEC 12

remote shell client (RSH), general description 12

remote shell daemon, general description, see also RSHD 12

reply messages, displaying banners 192

RES (Random Early Slowdown) 144

reset connection after system failure 114

resolver 70, 82, 92

Resolver setup file, updates by release 30

RESOLVER_IPNODES environment variable 58

RESOLVER_PROC SYS1.PARMLIB member 35

RESOLVER_TRACE environment variable 58

Resource ReSerVation Protocol (RSVP) Agent 10

RESTRICTAPPL 209

REXEC 12, 153

REXECD 12

REXX sockets 7

RFC (request for comment)

- list of 269

RFC (request for comments)

- accessing online xx

- RFC 2355 218
- RFC 2389 188
- RFC 2428 180
- RFC 2640 189
- RFC1323 130
- RIP1 and RIP2 packets 103
- rndc.conf file 250
- route display 163
- ROUTE PROFILE.TCPIP configuration statement, updates by release 33
- Route Trip Response Time (RTT) 130
- ROUTE/-r, Netstat 162
- routing over OSA-Express QDIO connection 117
- routing table, IP 162
- routing, client connections in sysplex distributor 135
- routing, IP 162
- RSH (remote shell client), general description 12
- RSHD 12
- RSHD Kerberos support, z/OS UNIX 111
- RSVP Agent 10
- RSVP API (RAPI) 16
- RTT (Route Trip Response Time) 130

S

- SACONFIG PROFILE.TCPIP configuration statement, updates by release 34
- SAFE command 173
- SAFE statement 170
- SAMEHOST 4
- SBSUB and SBSUBCHAR statement 170
- SBSUBCHAR 176
- scan detection 95
- SCANINTERVAL 205
- schema 139
- schema, policy 100
- SEARCH directive 92
- SEARCH TCPIP.DATA statement, updates by release 31
- secret-key cryptography 185
- Secure Sockets Layer, enhancements 223
- SECURE_* statements 169, 171
- SECUREPORT statement 223
- security and FRCA access control 70
- security zones 151
- security, catalog 182
- security, FTP server 181
- security, TLS enablement for FTP 184
- sequential LU name lookup 215
- server anonymous 194
- server bind control 151
- server security, FTP 181
- server, SOCKS 183
- servers, "middle tier" TN3270 155
- Service Level Agreement (SLA) subagent general description 233
- Service Level Policy Quality of Service (QoS) Enhancements 141
- service levels, QoS 112
- Service Manager 118
- SERVICEMGR keyword 119

- setsockopt and getsockopt API calls 108
- SEZAHHELP 65
- SEZALINK 35, 65
- SEZALOAD 35, 65
- shortcut keys 283
- SIMCLIENTLU 206
- Simple Mail Transfer Protocol (SMTP) exit, filtering unwanted mail 122
- simple mail transfer protocol, see also SMTP, general description 13
- Simple Network Time Protocol (SNTP) 73
- simulated limit mode 95
- SITE command 174, 187, 198, 199
- SITE subcommand 191
- SIZE command 197
- SLA Subagent 10
- SMF format type 118 121
- SMF format type 119 122
- SMF recording 121
- SMF records 194
- SMFCONFIG PROFILE.TCPIP configuration statement, updates by release 34
- SMFINIT 206
- SMFPRMxx parmliib member 122
- SMFTERM 206
- SMPTEXTIT 122
- SMTP (simple mail transfer protocol), general description 13
- SMTP exit to filter unwanted mail 122
- SMTPPROC application 122
- SNA extensions and TN3270E 218
- SNAEXT 206
- SNMP subagent support, OSA 72
- SNMP, general description 10
- SNMPD.CONF file 265
- SNMPTRAP.DEST file 266
- SNTP (Simple Network Time Protocol) 73
- SNTP, general description 10
- sntpd UNIX command, updates by release 57
- SOCKAPI 159
- socket addresses, AF_INET6 153
- socket API commands 87
- Socket API Trace 159
- socket APIs 59
- socket APIs, updates by release 58
 - enabled for IPv6 58
 - table showing updates from release to release 59
- Sockets Extended
 - definition of call instruction API 7
 - definition of macro API 7
- sockets listener, CICS 120
- sockets, fast local 160
- SOCKS server 183
- SOCKSCONFIGFILE 171, 180
- SORTLIST directive 92
- SORTLIST TCPIP.DATA statement, updates by release 31
- Source VIPAs for TCP connections, Sysplex-wide Dynamic 66
- SOURCEVIPAs 243
- spam, filtering with SMTP exit 122

SRESTART command 174
 SSL 224
 Stack Access Control 150
 start options, FTP command 174
 STAT command 174, 192
 statistics gathering mode 95
 Statistics mode (TRM) 143
 storage utilization and management, TCP/IP 124
 storage, QDIO or iQDIO 78
 stream mode restart 187
 subagent support, OSA SNMP 72
 subagent, OMPROUTE
 general description 233
 subagent, Service Level Agreement (SLA)
 general description 233
 subagent, TCP/IP
 general description 232
 substitution characters and FTP 175
 surrogate RACF support and password 183
 SWSA (Sysplex Wide Security Association) 68
 SYS1.PARMLIB members, updates by release 35
 BPXPRMxx member 35
 CTIEZB00 member 35
 CTIIDS00 member 35
 CTIRES00 member 35
 EZAIPCSP member 35
 IKJTSOxx member 35
 PROGxx member 35
 RESOLVER_PROC 35
 Syslogd 96
 SYSLOGD configuration file, updates by release 31
 syslogd Isolation 147
 syslogd UNIX command, updates by release 57
 SYSNAME 129
 sysObjectID 236
 sysplex distributor 135
 Sysplex Distributor 66
 Sysplex Distributor and Cisco's MNLB 118
 Sysplex Distributor and fast connection reset 114
 Sysplex Distributor policy enhancements 98
 Sysplex Wide Security Association (SWSA) 68
 Sysplex-wide Dynamic Source VIPAs for TCP
 connections 66
 SYSPLEXPORTS 67
 SYSTCPIS CTRACE 96
 System Management Facilities (SMF) recording 121
 system outages 138

T
 TCP (transmission control protocol), definition 2
 TCP connections, Sysplex-wide Dynamic Source VIPAs
 for 66
 TCP TIMESTAMP option 130
 TCP_NODELAY 108
 TCP/IP
 online information xx
 protocol specifications 269
 TCP/IP IPCS commands 159
 TCP/IP Macro API 159
 TCP/IP storage utilization management 124
 TCP/IP subagent
 general description 232
 TCP/IP tracing 160
 TCPCONFIG PROFILE.TCPIP configuration statement,
 updates by release 34
 TCPIP.DATA statements and parameters, updates by
 release 31
 TCPIPICS IPCS subcommand, updates by release 63
 TCPSTACKSOURCEVIPA 67
 Telnet Client Identifiers 219
 Telnet operator commands 209
 Telnet parameter placement 213
 Telnet parameters 204
 Telnet port qualification 211
 Telnet printer specification 212
 Telnet server and client 203
 Telnet wildcard capability 215
 TELNETGLOBALS 204
 TELNETPARMS information block 205
 TIMED 73
 TIMEMARK 205
 timer, FINWAIT2 configurable 130
 TIMESTAMP option, TCP 130
 TKOSPECLURECON 206
 TLS enablement for FTP 184
 TLS V1 protocol 215
 TLSTIMEOUT statement 169, 171
 TN3270 client reconnect to TN3270E server 226
 TN3270 DEBUG 228
 TN3270 diagnostics 217
 TN3270 Enhanced SLU simulation 225
 TN3270 Negotiated SSL 223
 TN3270 NQN Support for the TN3270E Server 226
 TN3270 profile 218
 TN3270 servers, "middle tier" 155
 TN3270 SSL 215, 224
 TN3270 Timemark Default Change 228
 TN3270E Resource Pooling 227
 token ring support, OSA-Express 127
 ToS (Type of Service) 112
 TRACE CT,ON,COMP= SYSTCPIP operator command,
 updates by release 42
 TRACE CT,ON,COMP= SYSTCPIS operator command,
 updates by release 42
 TRACE CT,ON,COMP= SYSTCPRE,SUB=
 (resolverprocname) operator command, updates by
 release 42
 trace formatter, CTRACE packet 113
 Trace option 217
 trace records 159
 trace records, segregating using syslogd 146
 trace, packet and data 87
 Traceroute 76
 traceroute UNIX command, updates by release 57
 TRACERTE 10
 TRACERTE TSO command, updates by release 49
 traces 72
 tracing TCP/IP 160
 tracing, syslogd 147
 trademark information 288
 traffic congestion, MPCIPA devices 143

- traffic control regulation 142
- traffic flow within networks 141
- Traffic Regulation and Management (TRM) 142
- Traffic Regulation Management (TRM) 95
- traffic regulation, UDP 95
- Transaction Request Message 120
- transferring MVS data sets with FTP URL 198
- transferring MVS load modules by using FTP 196
- TRANSFORM 206
- transmission control protocol (TCP), definition 2
- transport layer, z/OS Communications Server TCP/IP 5
- Trap Forwarder Daemon
 - general description 233
- trap, abend (Telnet) 217
- traps and SNMP, definition 232
- TRM (Traffic Regulation Management) 95
- TRM daemon 10
- TRM policy and modes 142
- trmd 96
- trmd UNIX command, updates by release 58
- trmdstat command 10
- trmdstat UNIX command, updates by release 58
- TSO commands, FTP z/OS UNIX and 171
- TSO commands, updates by release 43
 - DIG 43
 - HOMETEST 43
 - NETSTAT 43
 - PING 48
 - TRACERTE 49
- TSO Traceroute 76
- tunnels, GRE 119
- tunnels, IPSec 68
- Type of Service (ToS) 112

U

- UCOUNT FTP.DATA statement 198
- UCOUNT statement 170, 171
- UDP (user datagram protocol), general description 5
- UDP traffic regulation 95
- UNIX and TSO commands, FTP z/OS 171
- UNIX commands, updates by release 49
 - onetstat 50
 - oping 56
 - orouted 56
 - orshd 56
 - otracert 56
 - pagent 57
 - pasearch 57
 - ping 57
 - sntpd 57
 - syslogd 57
 - traceroute 57
 - trmd 58
 - trmdstat 58
- UNIX RSHD Kerberos support, z/OS 111
- unwanted mail, SMTP exit to filter 122
- user datagram protocol (UDP), general description 5
- user exits, FTP server 178

- user interface
 - ISPF 283
 - TSO/E 283
- user priorities 112
- user written exit 200
- user-level FTP server options 187

V

- V3 certificate, X509 221
- VARY DEBUG command 217
- VARY TCPIP,,DATTRACE operator command, updates by release 42
- VARY TCPIP,,PKTTRACE operator command, updates by release 42
- VARY TCPIP,,PURGECache operator command, updates by release 42
- VCOUNT FTP.DATA statement 198
- VCOUNT statement 170, 171
- VERBOSE command 174
- Version 1 and Version 2 policies 139
- VIPA non-disruptive takeover 138
- VIPA, Allow Source 243
- VIPA, Dynamic 119
- VIPABACKUP PROFILE.TCPIP configuration statement, updates by release 34
- VIPADEFINE PROFILE.TCPIP configuration statement, updates by release 34
- VIPADISTRIBUTE PROFILE.TCPIP configuration statement, updates by release 34
- VIPARANGE PROFILE.TCPIP configuration statement, updates by release 34
- VIPAs for TCP connections, Sysplex-wide Dynamic Source 66
- VIPASMPARMS PROFILE.TCPIP configuration statement, updates by release 34
- virtual LAN priority tagging 112
- VIRTUAL_LINK statement 107
- VOLUME FTP.DATA statement 198
- VOLUME statement 170, 171
- VTAM DISPLAY TRL command 143
- VTAM, online information xx

W

- web pages, processing static 161
- welcome page statements 168
- welcome page support 192
- wildcard capability, Telnet 215
- wildcard IP addressing for OMPROUTE 105
- WLM (workload manager) 162, 249
- WLM weight 98
- workload balancing 118, 135
- workload manager, see also WLM 162

X

- X Window System programming library 15
- X.25, support by SAMEHOST 4
- X509 V3 certificate 221

XPG4 standard
using z/OS UNIX C sockets API with 8

Z

z/OS UNIX RSHD Kerberos support 111
z/OS V1R2 Communications Server release
summary 91
z/OS V1R4 Communications Server release
summary 65
z/OS, documentation library listing xxiii
z/OS, listing of documentation available 279
zSeries, definition of 1

Communicating Your Comments to IBM

If you especially like or dislike anything about this document, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this document. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this document.
- If you prefer to send comments by FAX, use this number: 1-800-254-0206
- If you prefer to send comments electronically, use this network ID: `usib2hpd@vnet.ibm.com`

Make sure to include the following in your note:

- Title and publication number of this document
- Page number or topic to which your comment applies.

Readers' Comments — We'd Like to Hear from You

**z/OS Communications Server
IP Migration
Version 1 Release 4**

Publication No. GC31-8773-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>				

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>				
Complete	<input type="checkbox"/>				
Easy to find	<input type="checkbox"/>				
Easy to understand	<input type="checkbox"/>				
Well organized	<input type="checkbox"/>				
Applicable to your tasks	<input type="checkbox"/>				

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? Yes No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.



Fold and Tape

Please do not staple

Fold and Tape



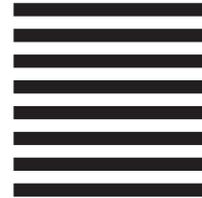
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Software Reengineering
Department G71A/ Bldg 503
Research Triangle Park, NC
27709-9990



Fold and Tape

Please do not staple

Fold and Tape



Program Number: 5694-A01 and 5655-G52

Printed in U.S.A.

GC31-8773-02



Spine information:



z/OS Communications Server

z/OS VIR4.0 CS: IP Migration

Version 1
Release 4