z/OS Communications Server

New Function Summary

Version 1 Release 12

GC31-8771-06

z/OS Communications Server

New Function Summary

Version 1 Release 12

GC31-8771-06

Note:
Before using this information and the product it supports, be sure to read the general information under "Notices" on page 119.

Seventh Edition (September 2010)

This edition applies to Version 1 Release 12 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments. You may send your comments to the following address.

International Business Machines Corporation
Attn: z/OS Communications Server Information Development
Department AKCA, Building 501
P.O. Box 12195, 3039 Cornwallis Road
Research Triangle Park, North Carolina 27709-2195

You can send us comments electronically by using one of the following methods:

Fax (USA and Canada):

1+919-254-1258

Send the fax to "Attn: z/OS Communications Server Information Development"

Internet e-mail:

comsvrcf@us.ibm.com

World Wide Web:

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

If you would like a reply, be sure to include your name, address, telephone number, or FAX number. Make sure to include the following in your comment or note:

- Title and order number of this document
- Page number or topic related to your comment

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.

Contents

Figures vii

Tables ix

About this document xi
Who should read this document xi
How this document is organized xi
How to use this document xii
Determining whether a publication is current xii
How to contact IBM service xiii
Conventions and terminology that are used in this document xiii
How to read a syntax diagram. xiv
Prerequisite and related information xvii
How to send your comments xxi

Summary of changes xxiii

Chapter 1. Planning to use new functions 1
Introduction to z/OS Communications Server 1
Determining which documents to use when migrating 2
IP encryption features 2
Planning checklist 3
TCP/IP packaging process. 4
MVS data sets 4
File system files 7
Defining SNA data sets 7
Data sets containing information for z/OS V1R12 Communications Server 10
Data sets containing information for NCP 18

Chapter 2. Roadmap to functions 21

Chapter 3. V1R12 new function summary 25
Application integration, data consolidation, and standards. 25
Enhancements to IPv6 router advertisement 25
Configurable default address selection policy table 26
Socket API support for source address selection 26
Resolver support for IPv6 connections to DNS name servers 27
Scalability, performance, constraint relief, and accelerators 28
Performance improvements for sysplex distributor connection routing. 28
Performance improvements for streaming bulk data 29
z/OS Communications Server in an ensemble 31
Extend sysplex distributor support for DataPower for IPv6 32
Improvements to AT-TLS performance 33
Sysplex distributor support for hot-standby server 33
Common storage reduction for TN3270E server 34
Performance improvements for fast local sockets 34
Improved resolver reaction to unresponsive DNS name servers 34
Sysplex autonomics monitoring TCP/IP abends 35
Security 35
IKE version 2 support 35
IPSec support for certificate trust chains and certificate revocation lists 37
IPSec support for cryptographic currency 38
IPSec support for FIPS 140 cryptographic mode 39
Trusted TCP connections 40

Digital certificate access server (DCAS) MODIFY command for debug level . . . 41
Simplification and consumability . . . 41
Enhancements to the TN3270E server . . . 41
IBM Health Checker for z/OS OMPROUTE checks . . . 42
Command to drop all connections for a server . . . 42
Control joining the sysplex XCF group . . . 43
Extension of the retry time limit for CSSMTP . . . 43
SNA and Enterprise Extender . . . 44
Enterprise Extender connection health verification . . . 44
Multipath control for Enterprise Extender . . . 45
Improved recovery from RTP pipe stalls . . . 45
Enhancements to topology database diagnostics . . . 45
System management and monitoring . . . 46
Performance improvement to TCP/IP callable NMI (EZBNMIFR) GetConnectionDetail request . . . 46
Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics . . . 46
SMF event records for sysplex events . . . 47
Management data for CSSMTP . . . 47
Data trace records for socket data flow start and end . . . 49
Enhancements to the TN3270E server - session manager sends CV64 . . . 49
Operator command to query and display OSA information . . . 50
Packet trace filtering for encapsulated packets . . . 50
Verify Netstat message catalog synchronization . . . 51
Enhancements to the TCP/IP storage display . . . 51
Enhancements to SNMP manager API . . . 51

Chapter 4. V1R11 new function summary . . . 53
Support considerations in V1R11 . . . 53
General release considerations in V1R11 . . . 53
Application integration, data consolidation, and standards . . . 53
New SMTP client for sending Internet mail . . . 54
FTP enhancements . . . 56
Customizable pre-logon banner for otelnetd . . . 63
Remote execution server enhancements . . . 63
TN3270 support of TSO logon reconnect . . . 64
IPv6 stateless address autoconfiguration enhancements . . . 64
New API to obtain IPv4 network interface MTU . . . 66
RFC 5095 deprecation of IPv6 type 0 route header . . . 66
CICS sockets enhancements . . . 67
Availability and business resilience . . . 67
Improved responsiveness to storage shortage conditions . . . 67
Disable moving DVIPA as source IP address . . . 68
Support for enhanced WLM routing algorithms . . . 68
Scalability, performance, constraint relief, and accelerators . . . 69
accept_and_receive API enhancements . . . 69
TCP/IP support for system z10 hardware instrumentation . . . 70
TCP/IP pathlength improvements . . . 70
TCP throughput improvements for high-latency networks . . . 71
Virtual storage constraint relief . . . 71
NSS private key and certificate services for XML appliances . . . 72
Enterprise Extender IPSec performance improvements . . . 72
Resolver DNS cache . . . 73
Sysplex autonomics improvements for FRCA . . . 74
QDIO routing accelerator . . . 74
Sysplex distributor enhancements . . . 75
OSA-Express3 optimized latency mode . . . 78
Security . . . 79
IPSec enhancements . . . 79
AT-TLS enhancements . . . 80
Simplification and consumability . . . 81
Configuration Assistant enhancements . . . 81
syslogd enhancements . . . 82

syslogd browser and search facilities . . . 82
Policy infrastructure management enhancements . . . 83
MVS console support for select TCP/IP commands . . . 85
IBM Health Checker for z/OS DNS server check . . . 85
SNA and Enterprise Extender . . . 86
Display potential model application name . . . 86
Include data space VIT with INOP dump . . . 86
HPR performance enhancements . . . 87
APPN topology database update enhancements . . . 90
Provide ACF/TAP as part of z/OS Communications Server . . . 91
System management and monitoring . . . 92
IBM Health Checker for z/OS RFC 4301 compliance. . . . 92
Network management enhancements . . . 92
Verbose Ping . . . 96
Virtualization . . . 96
QDIO enhancements for Workload Manager IO priority . . . 96
QDIO support for OSA interface isolation . . . 97

Appendix A. Related protocol specifications . . . 99
Internet drafts . . . 115

Appendix B. Accessibility . . . 117

Notices . . . 119
Policy for unsupported hardware. . . . 126
Trademarks . . . 127

Bibliography . . . 129

Index . . . 133

Communicating your comments to IBM . . . 139

Figures

1. Correlation between DD statement and NCP definition statement 19

Tables

1. Comparing documents used in migration . . . 2
2. Distribution library data sets . . . 4
3. Target library data sets . . . 5
4. Shared distribution and target library data sets . . . 6
5. z/OS data sets containing information for z/OS Communications Server . . . 7
6. z/OS data sets containing information for both VTAM and NCP . . . 9
7. IBM-supplied default values for CSM buffer pools . . . 15
8. Roadmap to functions . . . 21
9. Enhancements to IPV6 router advertisement . . . 25
10. Configurable default address selection policy table . . . 26
11. Socket API support for source address selection . . . 27
12. Resolver support for IPv6 connections to DNS name servers . . . 27
13. Performance improvements for sysplex distributor connection routing . . . 29
14. Performance improvements for streaming bulk data . . . 30
15. z/OS Communications Server in an ensemble . . . 32
16. Extend sysplex distributor support for DataPower for IPv6 . . . 33
17. Sysplex distributor support for hot-standby server . . . 33
18. Common storage reduction for TN3270E server . . . 34
19. Improved resolver reaction to unresponsive DNS name servers . . . 35
20. Enabling IKE version 2 support . . . 36
21. Using hash and URL encoding of certificates and certificate bundles . . . 36
22. IPSec support for certificate trust chains and certificate revocation lists . . . 38
23. IPSec support for cryptographic currency . . . 39
24. IPSec support for FIPS 140 cryptographic mode . . . 40
25. Trusted TCP connections . . . 40
26. Digital certificate access server (DCAS) MODIFY command for debug level . . . 41
27. Enhancements to the TN3270E server . . . 42
28. IBM Health Checker for z/OS OMPROUTE checks . . . 42
29. Command to drop all connections for a server . . . 43
30. Control joining the sysplex XCF group . . . 43
31. Extension of the retry time limit for CSSMTP . . . 43
32. Enterprise Extender connection health verification . . . 44
33. Multipath control for Enterprise Extender . . . 45
34. Enhancements to topology database diagnostics . . . 45
35. Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics . . . 47
36. SMF event records for sysplex events . . . 47
37. NMI enhancements - CSSMTP events using the NMI real-time SMF events . . . 48
38. CSSMTP and application data . . . 49
39. Data trace records for socket data flow start and end . . . 49
40. Enhancements to the TN3270E server - session manager sends CV64 . . . 50
41. Operator command to query and display OSA information . . . 50
42. Packet trace filtering for encapsulated packets . . . 51
43. Verify Netstat message catalog synchronization . . . 51
44. Enhancements to the TCP/IP storage display . . . 51
45. Enhancements to SNMP manager API. . . . 52
46. New SMTP client for sending Internet mail . . . 55
47. FTP access to UNIX named pipes . . . 57
48. FTP large-volume access . . . 61
49. FTP passive mode enhancements . . . 62
50. Customizable pre-logon banner for otelnetd. . . . 63
51. Remote execution server enhancements . . . 64
52. IPv6 stateless address autoconfiguration enhancements . . . 65
53. New API to obtain IPv4 network interface MTU . . . 66
54. Improved responsiveness to storage shortage conditions . . . 67
55. Support for enhanced WLM routing algorithms . . . 69

56. TCP throughput improvements for high-latency networks 71
57. Virtual storage constraint relief 72
58. NSS private key and certificate services for XML appliances 72
59. Resolver DNS cache. 73
60. QDIO routing accelerator 75
61. Sysplex distributor connection routing accelerator. 76
62. OSA-Express3 optimized latency mode 79
63. AT-TLS enhancements 80
64. Configuration Assistant enhancements 81
65. syslogd enhancements 82
66. syslogd browser and search facilities 83
67. Policy infrastructure management enhancements 83
68. MVS console support for select TCP/IP commands 85
69. IBM Health Checker for z/OS DNS server check 86
70. Display potential model application name 86
71. Include data space VIT with INOP dump 87
72. HPR performance enhancements coexistence PTF APARs 88
73. HPR performance enhancements 88
74. APPN topology database update enhancements 91
75. Provide ACF/TAP as part of z/OS Communications Server 91
76. IBM Health Checker for z/OS RFC 4301 compliance 92
77. NMI stack configuration data 93
78. Network management interface enhancements - detailed CSM usage 94
79. OSA network traffic analyzer data 95
80. NMI sysplex networking data 96
81. Verbose Ping 96
82. QDIO enhancements for WLM IO priority 97
83. QDIO support for OSA interface isolation 98

About this document

The purpose of this document is to describe the exploitation considerations of the new functions for the TCP/IP and SNA components of z/OS® Version 1 Release 12 Communications Server (z/OS Communications Server). It also includes the exploitation considerations of z/OS V1R11 Communications Server.

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.

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.

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

Who should read this document

This document is 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.

To use the IP functions described in this document, you need to be familiar with Transmission Control Protocol/Internet Protocol (TCP/IP) and the z/OS platform.

To use the SNA functions described in this document, you need to be familiar with the basic concepts of telecommunication, SNA, VTAM®, and the z/OS platform.

How this document is organized

This document contains these topics:

- Chapter 1, “Planning to use new functions,” on page 1 includes a brief introduction to z/OS Communications Server, information about hardware requirements, references to documents that will help you if you are migrating, information about the IP encryption features, a planning checklist, and data set information.

- Chapter 2, “Roadmap to functions,” on page 21 provides a roadmap of the functional enhancements introduced in z/OS V1R12 Communications Server and z/OS V1R11 Communications Server. Each entry indicates whether enabling or actions are required.
- Chapter 3, “V1R12 new function summary,” on page 25 summarizes the functions and migration considerations of z/OS V1R12 Communications Server.
- Chapter 4, “V1R11 new function summary,” on page 53 summarizes the functions and migration considerations of z/OS V1R11 Communications Server.
- Appendix A, “Related protocol specifications,” on page 99 lists the related protocol specifications for TCP/IP.
- "Architectural specifications" lists documents that provide architectural specifications for the SNA Protocol.
- "Accessibility" describes accessibility features to help users with physical disabilities.
- "Notices" contains notices and trademarks used in this document.
- "Bibliography" contains descriptions of the documents in the z/OS Communications Server library.

How to use this document

Use this document as a brief introduction to z/OS Communications Server and as an introduction to every function and enhancement of the current and most recent releases of z/OS Communications Server.

The roadmap shows you a list of the functions of the current and most recent releases. Use the roadmap to see a release at a glance and to determine which functions have tasks that are necessary to use the functions.

Use the function summary topics to learn about this information:

- A brief description of the function or enhancement
- Identification of the area that the function is designed to improve, such as customization or diagnosis
- Restrictions of the function, if any
- A task table identifying the actions necessary to use the function
- References to the documents that contain more detailed information

Determining whether 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 file name (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.

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-IBM-SERV). You will receive a return call within 8 business hours (Monday – Friday, 8:00 a.m. – 5:00 p.m., local customer time).

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

If you would like to provide feedback on this publication, see "Communicating your comments to IBM" on page 139.

Conventions and terminology that are used in this document

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

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

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

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

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

For definitions of the terms and abbreviations that are used in this document, you can view the latest IBM terminology at the IBM Terminology Web site.

Clarification of notes

Information traditionally qualified as **Notes** is further qualified as follows:

Note Supplemental detail

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

Guideline
Customary way to perform a procedure

Rule Something you must do; limitations on your actions

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

Requirement
Dependencies, prerequisites

Result Indicates the outcome

How to read a syntax diagram

This syntax information applies to all commands and statements that do not have their own syntax described elsewhere.

The syntax diagram shows you how to specify a command so that the operating system can correctly interpret what you type. Read the syntax diagram from left to right and from top to bottom, following the horizontal line (the main path).

Symbols and punctuation

The following symbols are used in syntax diagrams:

Symbol
Description

►► Marks the beginning of the command syntax.

► Indicates that the command syntax is continued.

| Marks the beginning and end of a fragment or part of the command syntax.

►◄ Marks the end of the command syntax.

You must include all punctuation such as colons, semicolons, commas, quotation marks, and minus signs that are shown in the syntax diagram.

Commands

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

- When describing how to use the command in a TSO environment, the command is presented in uppercase (for example, NETSTAT).
- When describing how to use the command in a z/OS UNIX environment, the command is presented in bold lowercase (for example, **netstat**).

Parameters

The following types of parameters are used in syntax diagrams.

Required
Required parameters are displayed on the main path.

Optional
Optional parameters are displayed below the main path.

Default
Default parameters are displayed above the main path.

Parameters are classified as keywords or variables. For the TSO and MVS console commands, the keywords are not case sensitive. You can code them in uppercase or lowercase. If the keyword appears in the syntax diagram in both uppercase and lowercase, the uppercase portion is the abbreviation for the keyword (for example, OPERand).

For the z/OS UNIX commands, the keywords must be entered in the case indicated in the syntax diagram.

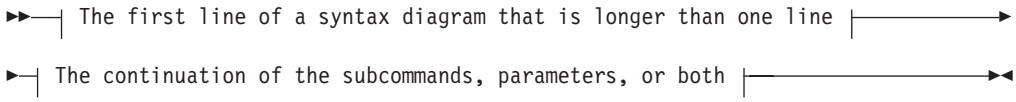
Variables are italicized, appear in lowercase letters, and represent names or values you supply. For example, a data set is a variable.

Syntax examples

In the following example, the USER command is a keyword. The required variable parameter is *user_id*, and the optional variable parameter is *password*. Replace the variable parameters with your own values.

Longer than one line

If a diagram is longer than one line, the first line ends with a single arrowhead and the second line begins with a single arrowhead.



Required operands

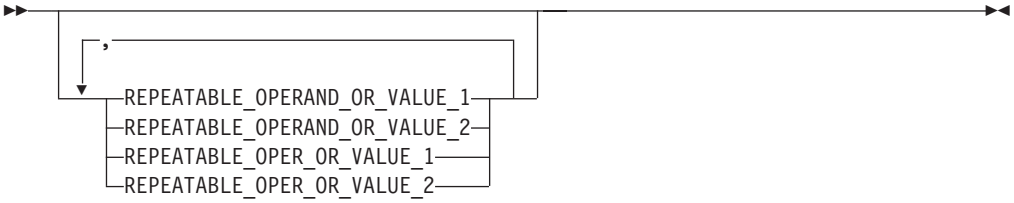
Required operands and values appear on the main path line. You must code required operands and values.

Optional values

Optional operands and values appear below the main path line. You do not have to code optional operands and values.

Selecting more than one operand

An arrow returning to the left above a group of operands or values means more than one can be selected, or a single one can be repeated.



Nonalphanumeric characters

If a diagram shows a character that is not alphanumeric (such as parentheses, periods, commas, and equal signs), you must code the character as part of the syntax. In this example, you must code OPERAND=(001,0.001).

Blank spaces in syntax diagrams

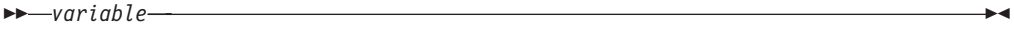
If a diagram shows a blank space, you must code the blank space as part of the syntax. In this example, you must code OPERAND=(001 FIXED).

Default operands

Default operands and values appear above the main path line. TCP/IP uses the default if you omit the operand entirely.

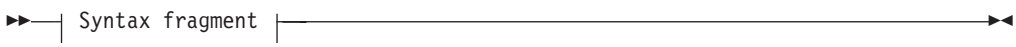
Variables

A word in all lowercase italics is a *variable*. Where you see a variable in the syntax, you must replace it with one of its allowable names or values, as defined in the text.



Syntax fragments

Some diagrams contain syntax fragments, which serve to break up diagrams that are too long, too complex, or too repetitious. Syntax fragment names are in mixed case and are shown in the diagram and in the heading of the fragment. The fragment is placed below the main diagram.



Syntax fragment:

Prerequisite and related information

z/OS Communications Server function is described in the z/OS Communications Server library. Descriptions of those documents are listed in "Bibliography" on page 129, in the back of this document.

Required information

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

Softcopy information

Softcopy publications are available in the following collections.

Titles	Order Number	Description
z/OS V1R12 Collection	SK3T-4269	This CD collection is shipped with the z/OS product. It includes the libraries for z/OS V1R12, in both BookManager and PDF formats.
z/OS Software Products Collection	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 *Getting Started with Parallel Sysplex*® bookshelf.
z/OS V1R12 and Software Products DVD Collection	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.
z/OS Licensed Product Library	SK3T-4307	This CD includes the licensed documents in both BookManager and PDF format.
IBM System z Redbooks Collection	SK3T-7876	The Redbooks® selected for this CD series are taken from the IBM Redbooks inventory of over 800 books. All the Redbooks that are of interest to the zSeries® platform professional are identified by their authors and are included in this collection. The zSeries subject areas range from e-business application development and enablement to hardware, networking, Linux®, solutions, security, parallel sysplex, and many others.

Other documents

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 following table lists documents that might be helpful to readers.

Title	Number
DNS and BIND, Fifth Edition, O'Reilly Media, 2006	ISBN 13: 978-0596100575
Routing in the Internet , Second Edition, Christian Huitema (Prentice Hall 1999)	ISBN 13: 978-0130226471
sendmail, Fourth Edition, Bryan Costales, Claus Assmann, George Jansen, and Gregory Shapiro, O'Reilly Media, 2007	ISBN 13: 978-0596510299
SNA Formats	GA27-3136
TCP/IP Illustrated, Volume 1: The Protocols, W. Richard Stevens, Addison-Wesley Professional, 1994	ISBN 13: 978-0201633467
TCP/IP Illustrated, Volume 2: The Implementation, Gary R. Wright and W. Richard Stevens, Addison-Wesley Professional, 1995	ISBN 13: 978-0201633542
TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols, W. Richard Stevens, Addison-Wesley Professional, 1996	ISBN 13: 978-0201634952
TCP/IP Tutorial and Technical Overview	GG24-3376
Understanding LDAP	SG24-4986
z/OS Cryptographic Services System SSL Programming	*SC24-5901*
z/OS Integrated Security Services LDAP Server Administration and Use	*SC24-5923*
z/OS JES2 Initialization and Tuning Guide	*SA22-7532*
z/OS Problem Management	*G325-2564*
z/OS MVS Diagnosis: Reference	*GA22-7588*
z/OS MVS Diagnosis: Tools and Service Aids	*GA22-7589*
z/OS MVS Using the Subsystem Interface	*SA22-7642*
z/OS Program Directory	*GI10-0670*
z/OS UNIX System Services Command Reference	*SA22-7802*
z/OS UNIX System Services Planning	*GA22-7800*
z/OS UNIX System Services Programming: Assembler Callable Services Reference	*SA22-7803*
z/OS UNIX System Services User's Guide	*SA22-7801*
z/OS XL C/C++ Run-Time Library Reference	*SA22-7821*
System z10, System z9 and zSeries OSA-Express Customer's Guide and Reference	*SA22-7935*

Redbooks

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

Title	Number
IBM z/OS V1R11 Communications Server TCP/IP Implementation, Volume 1: Base Functions, Connectivity, and Routing	SG24-7798
IBM z/OS V1R11 Communications Server TCP/IP Implementation, Volume 2: Standard Applications	SG24-7799
IBM z/OS V1R11 Communications Server TCP/IP Implementation, Volume 3: High Availability, Scalability, and Performance	SG24-7800
IBM z/OS V1R11 Communications Server TCP/IP Implementation, Volume 4: Security and Policy-Based Networking	SG24-7801
IBM Communication Controller Migration Guide	SG24-6298
IP Network Design Guide	SG24-2580
Managing OS/390® TCP/IP with SNMP	SG24-5866
Migrating Subarea Networks to an IP Infrastructure Using Enterprise Extender	SG24-5957
SecureWay™ Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements	SG24–5631
SNA and TCP/IP Integration	SG24-5291
TCP/IP in a Sysplex	SG24-5235
TCP/IP Tutorial and Technical Overview	GG24-3376
Threadsafe Considerations for CICS	SG24-6351

Where to find related information on the Internet

z/OS

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

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

z/OS Internet Library

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

www.ibm.com/systems/z/os/zos/bkserv/

IBM Communications Server product

The primary home page for information about z/OS Communications Server

http://www.software.ibm.com/network/commserver/

IBM Communications Server product support

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

http://www.software.ibm.com/network/commserver/support/

IBM Communications Server performance information

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

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

IBM Systems Center publications

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

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

IBM Systems Center flashes

Search the Technical Sales Library for Techdocs (including Flashes, presentations, Technotes, FAQs, white papers, Customer Support Plans, and Skills Transfer information)

http://www.ibm.com/support/techdocs/atsmastr.nsf

RFCs

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

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

Internet drafts

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

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

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

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

DNS Web sites

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

USENET news groups
comp.protocols.dns.bind

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

BIND Users

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

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

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

The z/OS Basic Skills Information Center

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

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

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

To access the z/OS Basic Skills Information Center, open your Web browser to the following Web site, which is available to all users (no login required): http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this document or any other z/OS Communications Server documentation, do one of the following:

- Go to the z/OS contact page at http://www.ibm.com/systems/z/os/zos/webqs.html. You can enter and submit your comments in the form provided at this Web site.
- Send your comments by e-mail to comsvrcf@us.ibm.com. Be sure to include the name of the document, the part number of the document, the version of z/OS Communications Server, and, if applicable, the specific location of the text that you are commenting on (for example, a section number, a page number or a table number).

Summary of changes

Summary of changes
for GC31-8771-06
z/OS Version 1 Release 12

This document contains information previously presented in GC31-8771-05, which supports z/OS Version 1 Release 11.

New information

Chapter 3, "V1R12 new function summary," on page 25 includes descriptions for the new functions and enhancements introduced in this release and explains how to use them. Entries for the new functions and enhancements are added to Chapter 2, "Roadmap to functions," on page 21.

Deleted information

- The release summary chapters for z/OS V1R10 are deleted and the V1R10 entries are deleted from Chapter 2, "Roadmap to functions," on page 21.

  You can still access the old release summary documentation at this 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.

You might notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

Summary of changes
for GC31-8771-05
z/OS Version 1 Release 11

This document contains information previously presented in GC31-8771-04, which supports z/OS Version 1 Release 10.

New information

Chapter 4, "V1R11 new function summary," on page 53 includes descriptions for the new functions and enhancements introduced in this release and explains how to use them. Entries for the new functions and enhancements are added to Chapter 2, "Roadmap to functions," on page 21.

Changed information

The IP and SNA sections are combined in chapters by release; they are no longer presented separately.

Deleted information

- The release summary chapters for z/OS V1R9 are deleted and the V1R9 entries are deleted from Chapter 2, "Roadmap to functions," on page 21.

  You can still access the old release summary documentation at this Web site: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/.

This document includes terminology, maintenance, and editorial changes.

Summary of changes
for GC31-8771-04
z/OS Version 1 Release 10

This document contains information previously presented in GC31-8771-03, which supports z/OS Version 1 Release 9.

New information

- Chapter 3. V1R10 IP new function summary includes descriptions and exploitation procedures for the new IP functions and enhancements introduced in this release. Entries for the new functions and enhancements are added to Chapter 2. Roadmap to IP functions.
- Chapter 6. V1R10 SNA new function summary includes descriptions and exploitation procedures for the new SNA functions and enhancements introduced in this release. Entries for the new functions and enhancements are added to Chapter 5. Roadmap to SNA functions.

Deleted information

- The release summary chapters for z/OS V1R8 are deleted. Likewise, the entries related to those releases are deleted from Chapter 2. Roadmap to IP functions and Chapter 5. Roadmap to SNA functions.

  You can still access the old release summary documentation at this Web site: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/.

This document includes terminology, maintenance, and editorial changes.

Chapter 1. Planning to use new functions

These topics help you plan to use new functions:

- "Introduction to z/OS Communications Server"
- "Determining which documents to use when migrating" on page 2
- "IP encryption features" on page 2
- "Planning checklist" on page 3
- "TCP/IP packaging process" on page 4
- "Defining SNA data sets" on page 7

Introduction to z/OS Communications Server

z/OS Communications Server is a network communication access method. It provides both Systems Network Architecture (SNA) and Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocols for z/OS.

The TCP/IP protocol suite (also called *stack*), includes associated applications, transport- and network-protocol layers, and connectivity and gateway functions. See *z/OS Communications Server: IP Configuration Guide* for more information about z/OS Communications Server IP protocols.

The SNA protocols are provided by VTAM and include Subarea, Advanced Peer-to-Peer Networking (APPN), and High Performance Routing protocols. z/OS Communications Server provides the interface between application programs residing in a host processor, and resources residing in an SNA network; it also links peer users in the network. See *z/OS Communications Server: SNA Network Implementation Guide* for more information about z/OS Communications Server SNA protocols.

For the purposes of this library, the following descriptions apply:

- The IBM zEnterprise™ System (zEnterprise) product line consists of the IBM zEnterprise 196 (z196).
- The IBM System z10™ product line includes IBM System z10® Enterprise Class (z10 EC) and the IBM System z10 Business Class (z10 BC).
- The IBM System z9® product line includes IBM System z9 Enterprise Class (z9® EC) (formerly known as the IBM System z9 109 [z9-109]), and the IBM System z9 Business Class (z9 BC).
- The IBM eServer™ zSeries product line includes the IBM eServer zSeries 990 (z990), 890 (z890), 900 (z900) and 800 (z800).
- The IBM System 390 (S/390®) product line includes the IBM S/390 Parallel Enterprise Server Generation 5 (G5) and Generation 6 (G6), and the IBM S/390 Multiprise 3000 Enterprise Server.

The z196, z10 EC, z10 BC, z9 EC (formerly z9-109), z9 BC, z990, z890, z900, and z800 servers are also known as z/Architecture® servers. z/OS V1R12 Communications Server runs only in z/Architecture mode on z/Architecture servers. The G5, G6, and Multiprise 3000 servers are not supported for z/OS V1R12 Communications Server.

Determining which documents to use when migrating

This table will help you determine which documents to use as you migrate.

Table 1. Comparing documents used in migration

z/OS Planning for Installation	This document helps you prepare to install z/OS or z/OS.e by giving you information you need to write an installation plan. To install means to perform the tasks necessary to make the system operational, starting with a decision to either install for the first time or upgrade, and ending when the system is ready for production. An installation plan is a record of the actions you need to take to install z/OS or z/OS.e. **Recommendation:** It is strongly recommended that you read this document. **Use this document as you prepare to install z/OS or z/OS.e.**
z/OS Migration	This document describes how to migrate (convert) from release to release. After a successful migration, the applications and resources on your new z/OS system will function the same way they did previously. **Use this document as a reference in keeping all z/OS applications working as they did in previous releases.**
z/OS Introduction and Release Guide	This document provides an overview of z/OS and lists the enhancements in each release. **Use this document to determine whether to obtain a new release and to decide which new functions to implement.**
z/OS Summary of Message and Interface Changes	This document describes the changes to interfaces for individual elements and features of z/OS. **Use this document as a reference to the new and changed commands, macros, panels, exit routines, data areas, messages, and other interfaces of individual elements and features of z/OS.**
z/OS Communications Server: New Function Summary	This document includes function summary topics to describe all the functional enhancements for the IP and SNA components of Communications Server, including task tables that identify the actions necessary to exploit new function. **Use this document as a reference to using all the enhancements of z/OS Communications Server.**

For an overview and map of the documentation available for z/OS, see the *z/OS Information Roadmap*.

IP encryption features

Encryption features are available for IP at no additional cost. Communications Server Security Level 3 is an optional unpriced feature and must be ordered.

The encryption features include these capabilities:

Level 1
This level of encryption is included in the base of z/OS V1R12 Communications Server.

Level 2
This level of encryption is included in the base of z/OS V1R12 Communications Server and offers IP security protocol (IPSec) DES and SNMPv3 56-bit DES.

Level 3

This level of encryption is included in the Communications Server Security Level 3 optional unpriced feature and offers IPSec Triple Data Encryption Standard (DES) and Advanced Encryption Standard (AES). AES includes the AES cipher-block chaining (AES-CBC) and AES Galois Counter (AES-GCM) modes.

Planning checklist

Migrating a z/OS Communications Server system from a previous release involves considerable planning. To familiarize yourself with the migration process, review this checklist. Tailor the checklist to meet the specific requirements of your installation.

__ 1. Understand your network topology, including the hardware and software in your network and your network configuration.

__ 2. Understand that z/OS V1R12 Communications Server is a base element of z/OS. Use the appropriate documents as you plan, migrate, and install:

For information about migration and writing an installation plan, see "Determining which documents to use when migrating" on page 2.

For information about installation, see these documents:

- *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

For information about storage requirements, see the *z/OS Program Directory*, IBMLINK, or z/OS Communications Server Support. You can also see the storage estimate worksheets in *z/OS Communications Server: SNA Network Implementation Guide*.

__ 3. Develop your education plan:
- Evaluate the z/OS V1R12 Communications Server features and enhancements by reading the new function summary topics in this document. Plan which new functions will be incorporated into your system.

__ 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. Get acquainted with the helpful information found at z/OS Communications Server Support.

__ 6. In writing a test plan for z/OS, include test cases for these items:
- TCP/IP applications
- Key or critical SNA applications and Original Equipment Manufacturer (OEM) software products.
- User-written applications such as: 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

__ 7. Back up your user exits and user modifications for later restore.

__ 8. Install z/OS Communications Server 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, see *z/OS Planning for Installation*.

__ 9. Complete post-installation activities:

- Use *z/OS Communications Server: IP Configuration Guide* to customize your TCP/IP system.
- Use the following to customize your SNA system:
  - *z/OS Communications Server: SNA Customization*
  - *z/OS Communications Server: SNA Network Implementation Guide*
  - *z/OS Communications Server: SNA Resource Definition Reference*
- Use *z/OS Migration* to determine migration actions.
- Reinstall user exits.
- Reinstall user modifications.
- Update operating procedures and automation routines.
- Activate new functions.

__ 10. Complete functional and stress tests.

TCP/IP packaging process

As a result of the installation process for z/OS V1R12 Communications Server, the product is 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 "File system files" on page 7.

MVS data sets

Table 2 lists the distribution library data sets required by z/OS V1R12 Communications Server.

Table 2. 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 include files
AEZAMODS	Distribution library for base link-edit modules
AEZARNT1	Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS
AEZARNT2	Reentrant object module for SEZAXAWL
AEZARNT3	Reentrant object module for SEZAXMLB
AEZAROE2	Reentrant object module for SEZAXAWL (z/OS UNIX support)
AEZAROE3	Reentrant object module for SEZAXMLB (z/OS UNIX support)
AEZARNT4	Reentrant object modules for RPC
AEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)

Table 2. Distribution library data sets (continued)

Data set	Description
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, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSMSG0	messages, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSPNL0	panels, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSTBL0	tables, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables

Table 3 lists the target library data sets required by z/OS V1R12 Communications Server.

Table 3. 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 SNMPIUCV subtask for the NetView® program, and the SQESERV module for the SNMP query engine
SEZADSIM	SNMP messages for the NetView program
SEZADSIP	SNMPIUCV initialization parameters for the NetView program
SEZAEXEC	CLISTs and REXX programs
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 LPALST
SEZAMENU	ISPF messages
SEZANCLS	NetView SNMP CLISTs
SEZANMAC	C headers and assembler macros for z/OS UNIX and TCP/IP Services APIs
SEZANPNL	NetView SNMP panels

Table 3. Target library data sets (continued)

Data set	Description
SEZAOLDX	X Window System library (X10 compatibility routines)
SEZAPENU	ISPF panels
SEZARNT1	Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS
SEZARNT2	Reentrant object module for SEZAXAWL
SEZARNT3	Reentrant object module for SEZAXMLB
SEZARNT4	Reentrant object modules for RPC
SEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)
SEZAROE2	Reentrant object module for SEZAXAWL (z/OS UNIX support)
SEZAROE3	Reentrant object module for SEZAXMLB (z/OS UNIX support)
SEZARPCL	Remote procedure call library
SEZATCP	Executable load modules for STEPLIB or LNKLST concatenation
SEZATCPX	Source for the country SBCS translation tables
SEZATELX	Source for the TELNET country translation tables
SEZAXAWL	Athena widget set
SEZAXLD1	Translated default tables
SEZAXLD2	Translated Kanji, Hangeul, and Traditional Chinese DBCS default tables and DBCS codefiles for TELNET transform mode
SEZAXMLB	Motif widget set
SEZAXTLB	X Window System Toolkit library
SEZAX11L	X Window System library

Table 4 lists the shared distribution and target library data sets required by z/OS V1R12 Communications Server.

Table 4. Shared distribution and target library data sets

Data set	Description
SYS1.CSSLIB	Interface routines for accessing callable services
SYS1.HELP	TSO help files
SYS1.MIGLIB	z/OS Communications Server formatted dump routines for the interactive problem control system (IPCS) and the z/OS Communications Server VIT Analysis Tool module, ISTRAFT1, which is used for problem diagnosis
SYS1.MSGENU / SYS1.AMSGENU	English-language message tables used by the MVS message service (MMS)
SYS1.NUCLEUS	Resident SVCs, callable services tables, and abnormal termination modules
SYS1.PARMLIB / SYS1.APARMLIB	IBM-supplied and installation-created members, which contain lists of system parameter values
SYS1.SAXREXEC	Contains system REXX programs
SYS1.SBLSCLI0	IPCS REXX execs and CLISTs
SYS1.SBLSKEL0	ISPF skeletons for the IPCS dialog

Table 4. Shared distribution and target library data sets (continued)

Data set	Description
SYS1.SBLSMSG0	ISPF messages for the IPCS dialog
SYS1.SBLSPNL0	ISPF panels for the IPCS dialog
SYS1.SBLSTBL0	ISPF tables for the IPCS dialog

File system files

See *z/OS UNIX System Services Planning* and *z/OS UNIX System Services User's Guide* for a description of the file system files.

Defining SNA data sets

This section describes z/OS data sets that you need to define or modify for z/OS V1R12 Communications Server. Table 5 shows the z/OS data sets that contain information for z/OS V1R12 Communications Server, and Table 6 on page 9 shows the z/OS data sets that contain information for both VTAM and NCP.

Enterprise Extender requires IP dataset definitions in addition to the SNA data sets. See *z/OS Communications Server: IP Configuration Guide* for more information.

These tables show the data sets and the approximate storage requirements for any new data sets and for any existing data sets whose requirements might have changed since your last installation.

Table 5. z/OS data sets containing information for z/OS Communications Server

Name of data set	Contents	Comments
SYS1.DSDB1	Data files of APPN directory information	Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes.
SYS1.DSDB2	Data files of APPN directory information	Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes.
SYS1.DSDBCTRL	Current status of SYS1.DSDB1 and SYS1.DSDB2	Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes.
SYS1.DUMPxx	Records of SVC DUMP	Required for diagnosis.
SYS1.LINKLIB	z/OS Communications Server initialization module, ISTINM01, which is used when z/OS Communications Server is started	Required.
	Logon manager load modules	Required for logon manager.
SYS1.LOGREC	z/OS Communications Server error records	Required.

Table 5. z/OS data sets containing information for z/OS Communications Server (continued)

Name of data set	Contents	Comments
SYS1.LPALIB	z/OS Communications Server load modules and user-written exit routines to be loaded into the shared link pack area	Required.
SYS1.MACLIB	z/OS Communications Server application program interface macros	Required.
SYS1.MIGLIB	z/OS Communications Server formatted dump routines for the interactive problem control system (IPCS) and the z/OS Communications Server VIT Analysis Tool module, ISTRAFT1, which is used for problem diagnosis	Required.
SYS1.NUCLEUS	z/OS Communications Server resident SVCs and abnormal termination modules	Required.
SYS1.PARMLIB	IBM-supplied and installation-created members, which contain lists of system parameter values	Required. This may also be a data set in the logical parmlib concatenation.
SYS1.PROCLIB	JCL for started tasks	Required for logon manager.
SYS1.SBLSCLI0	IPCS REXX execs and CLISTs	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures* for more information.
SYS1.SBLSKEL0	ISPF skeletons for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures* for more information.
SYS1.SBLSMSG0	ISPF messages for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures* for more information.
SYS1.SBLSPNL0	ISPF panels for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures* for more information.
SYS1.SBLSTBL0	ISPF tables for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis.
SYS1.SISTASGD	ASN.1 and GDMO syntax data sets	Included for reference by CMIP services application programmers.
SYS1.SISTASN1	Contains two categories of data set members: • ACYPRES: List of abstract syntax notation 1 (ASN.1) definition data sets. This is a member of a partitioned data set. • The members listed in ACYPRES.	Required for CMIP services. See "SYS1.SISTASN1" on page 11 for a description.
SYS1.SISTCLIB	z/OS Communications Server load modules to be loaded into common service area and extended common service area (CSA/ECSA) storage	Required.

Table 5. z/OS data sets containing information for z/OS Communications Server (continued)

Name of data set	Contents	Comments
SYS1.SISTCMIP	Directory definition file. The member name of the directory definition file is ACYDDF.	Required for CMIP services. See "SYS1.SISTCMIP" on page 11 for a description.
SYS1.SISTDAT1	Online tools	Optional. Use this library only if you intend to use the online information tools included with z/OS Communications Server.
SYS1.SISTDAT2	Message skeleton file for translation	Required. See *z/OS Communications Server: SNA Network Implementation Guide*.
SYS1.SISTGDMO	Compiled definitions for the ISO standard, Guidelines for the Definition of Managed Objects (GDMO). This is a partitioned data set consisting of one member, ACYGDMO.	Required for CMIP services. Member name ACYGDMO must be included on the DD statement for SISTGDMO in the VTAM start procedure: //ACYGDMO DD SYS1.SISTGDMO(ACYGDMO),DISP=SHR.
SYS1.SISTMAC1	z/OS Communications Server macros used to build user tables and parameter lists to build installation exits	Required.
SYS1.TRACE	GTF trace records	Required to run external trace. **Note:** For information about using multiple SYS1.TRACE data sets, see the *z/OS MVS Diagnosis: Tools and Service Aids*.
SYS1.TRSDB	Network topology database	Required for APPN topology database checkpointing function; must be allocated before initialization. This data set cannot be allowed to span multiple volumes.
Dynamic I/O configuration data sets	Dynamically created definitions of devices with all associated LUs	Optional; includes USER1.AUTO.VTAMLST and a catalog entry checkpoint data set. Required for dynamic I/O configuration.

Table 6 shows the z/OS data sets that contain VTAM information and NCP information if there is an NCP owned by that VTAM.

Table 6. z/OS data sets containing information for both VTAM and NCP

Name of data set	Contents	Comments
SYS1.ASAMPLIB	Sample of network operator command table and sample JCL for installation	Required for installation. Provided by IBM.
SYS1.SAMPLIB	Alterable copy of sample network operator command table, sample JCL for installation, and command lists for dynamic I/O	Required for installation. Provided by IBM.

Table 6. z/OS data sets containing information for both VTAM and NCP (continued)

Name of data set	Contents	Comments
SYS1.SSPLIB	NCP loader utility program	Required; added when NCP is installed. See "SYS1.SSPLIB" on page 19 for information on SYS1.SSPLIB requirements.
	NCP dump utility program	Required; added when NCP is installed. See "SYS1.SSPLIB" on page 19 for information on SYS1.SSPLIB requirements.
	NCP dump bootstrap program	Required; added when NCP is installed. See "SYS1.SSPLIB" on page 19 for information on SYS1.SSPLIB requirements.
SYS1.VTAMLIB	• Load modules for z/OS Communications Server • User-defined tables, default tables, and exit routines	Only z/OS Communications Server load modules are required. Must be listed in an IEAAPFxx parmlib member.
SYS1.VTAMLST	z/OS Communications Server definition statements and start options	Required; created by user before starting z/OS Communications Server. You can modify this data set, but you need to be very careful about the relationship between z/OS Communications Server and NCP definition statements. For example, changing a VTAMLST member without changing a corresponding NCP definition statement can cause serious errors that are difficult to diagnose.
Configuration restart data sets	z/OS Communications Server status of minor nodes for each major node	Required if a warm restart is to be used. Created by user before starting z/OS Communications Server.
SYS1.NODELST	z/OS Communications Server status of major nodes	Required if restart of all previously active major nodes is desired.
NCP load library	NCP load modules	Each NCP stored as a separate member of library. Created during NCP generation. Must be an APF-authorized library.
NCP dump data set	Dump records for NCP	Required if z/OS Communications Server is requested to provide a dump of NCP. Created by user before starting z/OS Communications Server.
SYS1.LDRIOTAB	Dump records for loader channel I/O trace	Required to hold loader channel I/O trace dumps. Created by user before starting z/OS Communications Server.
CSP and MOSS dump data set	Dump records for CSP and MOSS	Required if z/OS Communications Server is requested to provide a dump of CSP or MOSS and if the user wants to store the CSP or MOSS dump in a unique data set. Created by user before starting z/OS Communications Server.

Data sets containing information for z/OS V1R12 Communications Server

This section describes data sets that contain information for z/OS V1R12 Communications Server.

SYS1.SISTCLIB

SYS1.SISTCLIB contains the z/OS Communications Server modules to be loaded into common service area and extended common service area (CSA/ECSA) storage.

To prepare the SYS1.SISTCLIB data set, do these steps:

1. Allocate the SYS1.SISTCLIB data set using a utility program, and catalog the data set before SMP/E installation. See the installation JCL sample ISTJEXAL in the *z/OS Program Directory* for a sample job using the IEFBR14 program to allocate SYS1.SISTCLIB.
2. Add a DD card for SYS1.SISTCLIB in the VTAM NET procedure as follows:

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

3. Define SYS1.SISTCLIB as an authorized library (a library listed in the currently used IEAAPF*xx*).

SYS1.SISTCMIP

SYS1.SISTCMIP contains the IBM-supplied CMIP directory definition file (with the DD name ISTCMIP), which you can edit to restrict access to CMIP services.

The LRECL for this file is 80.

The file is loaded when CMIP services is started and can be reloaded using the **MODIFY TABLE** command. Start CMIP services using one of these methods:

- Issue the **MODIFY VTAMOPTS** command with the **OSIMGMT=YES** operand.
- Start z/OS Communications Server with the **OSIMGMT=YES** start option.

If CMIP services is active, edit the directory definition file and then load it by issuing the **MODIFY TABLE** command:

```
MODIFY proc,TABLE,OPT=LOAD,TYPE=CMIPDDF
```

SYS1.SISTASN1

The LRECL for this file is 1024.

SYS1.VTAMLST

SYS1.VTAMLST is the z/OS Communications Server definition library, which consists of files containing the definitions for network resources and start options. It is a required partitioned data set, and you need to allocate it on a direct-access volume before you file z/OS Communications Server network definitions.

This data set can be allocated and cataloged at either of these times:

- Any time before its initial use. Run the IEHPROGM utility program or the IEBUPDTE utility program.
- When the data set is first used. Code the appropriate job control language (JCL).

To prepare the SYS1.VTAMLST data set, do these steps:

1. Allocate space to accommodate the filing of definitions for major nodes and anticipated sets of start options. The amount needed depends on the number of nodes and operands used and on the number of start options. See *z/OS Communications Server: SNA Network Implementation Guide* for more information about start options.
2. Specify the DD name for SYS1.VTAMLST as VTAMLST. You should specify these DCB subparameters:

   ```
   RECFM=FB,LRECL=80,BLKSIZE=any multiple of 80
   ```

3. Code **LABEL=RETPD=0** on all DD statements for SYS1.VTAMLST. If you do not, an operator awareness message requiring a reply might be generated.
4. If you generate a NEWDEFN data set as part of NCP generation processing, ensure that it is loaded into SYS1.VTAMLST prior to activating the NCP. Failure to do so can cause serious problems. z/OS Communications Server uses the NCP source, in addition to the NCP load module and RRT, when loading and activating communication controllers. SYS1.VTAMLST must contain either the source used as input to the NCP generation process, if a NEWDEFN data set was not created, or the NEWDEFN data set, if one was created. For more information about NEWDEFN, see *NCP, SSP, and EP Generation and Loading Guide*.
5. If you are configuring z/OS Communications Server as an APPN node (or plan to do so in the future), copy the IBM-supplied APPN class of service (COS) definitions and APPN transmission group (TG) profiles from ASAMPLIB into SYS1.VTAMLST. Three sets of IBM-supplied COS definitions are available to enable z/OS Communications Server to select an optimal route for a session:
   - COSAPPN

     The definitions in COSAPPN are appropriate for most sessions.
   - ISTACST2

     The definitions in ISTACST2 are most useful for multiple types of connections with different TG characteristics. For example, the definitions are useful when channel-to-channel, token ring network, FDDI LAN, or ATM are used in the network.
   - ISTACST3

     The definitions in ISTACST3 are designed to enable z/OS Communications Server to select an optimal route for a session when connections used in the network include those with high speed link characteristics such as FICON®, Gigabit Ethernet, and HiperSockets™.

   One of these three sets of APPN COS definitions is required if z/OS Communications Server is configured as an APPN node. To use COSAPPN, ISTACST2, or ISTACST3, you must copy the appropriate set of definitions into SYS1.VTAMLST at z/OS Communications Server installation, and then activate the member in which the definitions reside. You can copy more than one set of definitions into SYS1.VTAMLST, but you can have only one set active at any time. For additional information about selecting and activating the best APPN COS definitions for your network, see the discussion about the IBM-supplied default classes of service in *z/OS Communications Server: SNA Network Implementation Guide*.

   The IBM-supplied TG profiles are in IBMTGPS in ASAMPLIB. IBMTGPS is not required, but you should include it. You can copy IBMTGPS into SYS1.VTAMLST; it is automatically activated when z/OS Communications Server is initialized.

Guidelines:

1. Because CP-CP session paths might include subarea VRs, it is also strongly recommended that you update your logon mode tables (including the IBM-supplied logon mode table, ISTINCLM) to include an appropriate COS= value on the CPSVCMG and CPSVRMGR mode table entries. Otherwise, a blank COS name will be used to determine the subarea VR and transmission priority that will be used for the VR portion of the CP-CP session path.
2. You can modify SYS1.VTAMLST, but you need to be very careful about the relationship between z/OS Communications Server and NCP definition

statements. For example, changing a VTAMLST member without changing a corresponding NCP definition statement can cause serious errors that are difficult to diagnose.

SYS1.VTAMLIB

SYS1.VTAMLIB is the z/OS Communications Server load module library, which consists of files containing the user tables, exit routines, and replaceable constants. It is a required partitioned data set.

SYS1.VTAMLIB is used to store these user tables:

- Class of service (COS) table
- Communication network management (CNM) routing table

  Note: SYS1.LPALIB can no longer be used to store the CNM routing table.
- Interpret table containing logon descriptions and any installation-coded logon routines in this table
- Logon mode table
- Session awareness (SAW) data filter table
- Unformatted system services table

Code the DD name for SYS1.VTAMLIB as VTAMLIB. You should specify these subparameters on the DCB parameter, with BLKSIZE specified as full-track blocking relative to the capacity of your direct access storage device (DASD):

```
RECFM=U,BLKSIZE=
```

Define SYS1.VTAMLIB as an authorized library (a library listed in the currently used IEAAPF*xx*).

Parmlib member for Communication Storage Manager (CSM)

The IVTPRM00 parmlib member sets parameters for CSM storage. IVTPRM00 is read during CSM initialization as a result of the first issuance of the IVTCSM REQUEST=CREATE_POOL macro. (z/OS Communications Server issues this macro when started.) These definitions can also be changed without requiring a re-IPL by editing the IVTPRM00 member and issuing the MODIFY CSM command without specifying the parameters on the command.

The parameter member IVTPRM00 can be found in:

- A data set defined by the PARMLIB DD statement in the TSO start procedure
- A data set in the logical parmlib concatenation
- SYS1.PARMLIB

IVTPRM00 has this format:

```
column |...+....1....+....2....+....3....+....4....+...

       FIXED MAX(maxfixK|M)

       ECSA MAX(maxecsaK|M)

       [POOL(bufsize, bufsource, initbuf, minfree, expbuf)]
```

Rules:

1. Each line in IVTPRM00 must start in column one.

2. FIXED and MAX or ECSA and MAX keywords must be separated by one or more spaces. It must be completed with its values on the same line.

The first two lines in the CSM parmlib member define the maximum amount of storage to be dedicated to fixed and ECSA buffers in CSM. Note that the fixed maximum represents the total fixed storage above and below the 2-gigabyte bar. You can also specify one POOL definition for each CSM buffer pool of a particular *bufsize* and *bufsource* combination. If parameters are not provided for a given CSM buffer pool, the IBM-supplied default values are used unless a program has provided these values on an IVTCSM REQUEST=CREATE_POOL macro.

This describe the variable fields in the CSM parmlib member:

maxfix A decimal integer specifying the maximum bytes of fixed storage to be dedicated for use by CSM. The range is from 1024K to 30720M. The default is 100M.

maxecsa A decimal integer specifying the maximum bytes of ECSA storage to be dedicated for use by CSM. The range is from 1024K to 2048M. The default is 100M.

Note: The *maxecsa* value should be less than 90% of the ECSA available on the z/OS system. CSM adjusts the *maxecsa* value to 90% of the system ECSA value and issues the message IVT5590I when the *maxecsa* value configured is larger than 90% of the ECSA available on the system.

K Denotes size in kilobytes

M Denotes size in megabytes.

bufsize Specifies the size of the buffers in the pool to be created. Valid pool sizes are 4K, 16K, 32K, 60K and 180K. *bufsize* is required for each POOL definition.

bufsource Specifies the storage source from which buffers are allocated. The values for *bufsource* are:

ECSA Buffers are allocated from ECSA storage.

DSPACE
Buffers are allocated from data space storage.

The *bufsource* variable is required for each POOL definition.

expbuf Specifies the number of buffers by which the pool is expanded when the number of free buffers falls below the *minfree* value. The valid ranges for each CSM buffer pool size are as follows:

Bufsize	Range for Expbuf
4K	1–256
16K	1–256
32K	1–128
60K	1–68
180K	1–22

The *expbuf* variable is required for each POOL definition.

initbuf Specifies the initial number of buffers to be created in the pool

when the first IVTCSM REQUEST=CREATE_POOL macro is issued by an application. If this value is specified as 0, only the base pool structure is created. In this case, the pool will be expanded on the first IVTCSM REQUEST=GET_BUFFER based on the specification for *expbuf*. The pool will not contract below the level specified by either *initbuf* or *expbuf*, whichever is higher.

The range for *initbuf* is 0–9999. If *initbuf* is omitted, the IBM-supplied default value is used unless overridden by an application's CREATE_POOL request.

minfree Specifies the minimum number of buffers to be free in the pool at any time. The storage pool will be expanded if the number of free buffers falls below this limit. The range for *minfree* is 0–9999. If *minfree* is omitted, the IBM-supplied default value is used unless overridden by an application's CREATE_POOL request.

Table 7 shows the IBM-supplied default values for *expbuf*, *initbuf*, and *minfree* for the CSM buffer pools.

Table 7. IBM-supplied default values for CSM buffer pools

Bufsize	**4 KB**	**16 KB**	**32 KB**	**60 KB**	**180 KB**
INITBUF	64	32	16	16	2
MINFREE	8	4	2	2	1
EXPBUF	16	8	4	4	2

z/OS system symbols can be used in IVTPRM00. See *z/OS Communications Server: SNA Network Implementation Guide* for more information about this function.

IBM Health Checker for z/OS can be used to check whether appropriate values are defined for the maximum amount of storage to be dedicated to fixed buffers and ECSA buffers in CSM. For more details about IBM Health Checker for z/OS, see IBM Health Checker for z/OS in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*.

APPN checkpointing data sets

These data sets are used when z/OS Communications Server is defined as a network node or interchange node, and are required for the APPN checkpointing function. These data sets cannot be allowed to span multiple volumes.

- SYS1.DSDB1
- SYS1.DSDB2
- SYS1.DSDBCTRL
- SYS1.TRSDB

SYS1.DSDB1 and SYS1.DSDB2 contain APPN directory information that is used to initialize the directory database when z/OS Communications Server is restarted.

Directory database information is stored alternately between SYS1.DSDB1 and SYS1.DSDB2. The directory database information is written to one of the data sets whenever a **MODIFY CHKPT TYPE=ALL** or **TYPE=DIR, HALT**, or **HALT QUICK** command is issued.

Not all of the resources from the directory database are written to the data sets when there is a checkpoint. The resources that are written to the data sets are those that satisfy these requirements:

- Targeted by a search
- Have a dynamic entry type that is not registered
- Updated within a period of time specified by the **DIRTIME** start option

The resources that are registered to the database at startup through resource registration and definition are not included in the checkpointed information.

SYS1.DSDBCTRL contains the current status of SYS1.DSDB1 and SYS1.DSDB2. It is read by z/OS Communications Server during initialization to determine whether SYS1.DSDB1 or SYS1.DSDB2 will be used to load the APPN directory database.

SYS1.TRSDB is required for checkpointing the network topology database. The information in this data set is used to initialize the network topology database whenever z/OS V1R12 Communications Server is restarted. The network topology database is written to this file whenever a **MODIFY CHKPT TYPE=TOPO** or **TYPE=ALL, HALT**, or **HALT QUICK** command is issued.

The APPN checkpointing data sets should be allocated and cataloged prior to z/OS Communications Server initialization. To prepare the APPN checkpointing data sets, do these tasks:

- Specify the DD name for SYS1.DSDB1 as DSDB1, for SYS1.DSDB2 as DSDB2, for SYS1.DSDBCTRL as DSDBCTRL, and SYS1.TRSDB as TRSDB.
- Specify these DCB subparameters for SYS1.DSDB1, SYS1.DSDB2, and SYS1.TRSDB:

  ```
  RECFM=FB,LRECL=1000,BLKSIZE=any multiple of 1000,DSORG=PS
  ```

- Specify these DCB subparameters for SYS1.DSDBCTRL:

  ```
  RECFM=FB,LRECL=20,BLKSIZE=20,DSORG=PS
  ```

Notes:

1. It is recommended that you not modify any of the foregoing data sets.
2. The DSDBCTRL is a fixed, 20-byte file; it requires a 20-byte block.

   Regarding DSDB1 and DSDB2: Every thousand resources to be checkpointed occupies 35 logical records, or six 6KB blocks of space; the only resources to be checkpointed are the cache DLU entries found during the search.
3. z/OS Communications Server fails the initial load of the network topology database if the checkpointed data set of another node is used, or the **SSCPNAME** operand is changed between the two IPLs. Should the initial load fail, z/OS Communications Server can acquire the information dynamically using TDUs.

Configuration restart data sets

If you want to use the z/OS Communications Server configuration restart facility, define configuration restart Virtual Storage Access Method (VSAM) data sets. See *z/OS Communications Server: SNA Network Implementation Guide* for a description of the configuration restart support.

To set up data sets for the major nodes that you will be using with configuration restart, do these steps:

1. Use a DD statement to define a configuration restart VSAM data set for each major node. The *ddname* must match the *ddname* on the **CONFGDS** operand of either the **PCCU** definition statement for the associated NCP or the **VBUILD**

definition statement for the associated major node. There are no z/OS Communications Server restrictions on this data set name.

This example defines a catalog entry to allocate space for a VSAM data set to contain the configuration restart data:

```
DEFINE
  CLUSTER(NAME(RESTART) -
          VOL(PUBLIC) -
          KEYS(18 0) -
          DATA(NAME(RESTART.DATA) -
          RECORDS(200 20) -
          RECORDSIZE(46 158)) -
  INDEX(NAME(RESTARTI.INDEX) -
          TRACKS(1))
```

2. Code the **INDEX** operand on the **DEFINE** command, or let it default. (See the sample **DEFINE** command.) The data set must be indexed.
3. Code **KEYS** (18 0). A key length of 18 bytes and an offset of 0 bytes are required.
4. Code **RECORDSIZE** (46 158). The average record size must be 46 bytes, and the maximum record size must be 158 bytes.
5. Make sure that the number of records in the file is equal to the number of minor nodes defined in the major node. When you choose the number of records for a switched major node, include each **PATH** definition statement. Therefore, the primary allocation should be the number of minor nodes in the major node, and the secondary allocation should be about 0.1 times the number of minor nodes.
6. When you change a major node definition in SYS1.VTAMLST, do not use the **WARM** start option when activating the new definition for the first time.

Dynamic configuration data sets for channel-attached devices

You can dynamically configure channel-attached devices in your network. See *z/OS Communications Server: SNA Network Implementation Guide* for a full description of this support.

To prepare your system to support dynamic configuration of channel-attached devices, complete these steps during your installation:

1. Define USER1.AUTO.VTAMLST as a partitioned data set. You can customize the name of the data set by altering its name in the ISTDEFIN command list. A sample of ISTDEFIN is found in SYS1.SAMPLIB.
2. Concatenate the USER1.AUTO.VTAMLST data set to the SYS1.VTAMLST data set as defined on the VTAMLST DD statement in the z/OS Communications Server start procedure. You also need to code the AUTO.VTAMLST data set as shared (DISP=SHR).

   ```
   ⋮
   //VTAMLST  DD DSN=SYS1.VTAMLST,DISP=SHR
              DD DSN=USER1.AUTO.VTAMLST,DISP=SHR
   ⋮
   ```

   USER1.AUTO.VTAMLST is used by ISTDEFIN for storing automatically generated major nodes. Each member of USER1.AUTO.VTAMLST representing a data host will then contain the definition for just one device. A local SNA major node will also include any of its associated LUs.
3. Set the data set control block (DCB) information for this data set with the same values as for the other VTAMLST data sets.
4. Define a catalog entry checkpoint data set (AUTOCKPT) for dynamic configuration support:

```
DEFINE
  CLUSTER(NAME('VSAM.AUTOCKPT') -
          VOL(PUBLIC) -
          KEYS(4 0) -
          DATA(NAME('VSAM.AUTOCKPT.DATA')-
          RECORDS(200 20) -
          RECORDSIZE(24 136)) -
  INDEX(NAME(VSAM.AUTOCKPT.INDEX) -
          TRACKS(1))
```

5. Add this data set using the AUTOCKPT DD statement in the z/OS Communications Server start procedure:

```
⋮
//AUTOCKPT DD DSN=VSAM.AUTOCKPT,AMP=AMORG,DISP=OLD
⋮
```

First Failure Support Technology

First Failure Support Technology™ (FFST™) helps you diagnose software problems by capturing information about a potential problem when it occurs.

NODELST data set

You can define a NODELST data set to maintain a list of major nodes that are active at one time. If you use the NODELST facility, you need to define VSAM data sets. See *z/OS Communications Server: SNA Network Implementation Guide* for more information on how NODELST is used.

To define a NODELST data set, perform these steps:

1. Use the **DEFINE** command to define a catalog entry and allocate space for an indexed cluster:

```
DEFINE
  CLUSTER(NAME(NODLST1) -
          VOL(PUBLIC) -
          KEYS(2 0) -
          DATA(NAME(NODLST1.DATA) -
          RECORDS(120 20) -
          RECORDSIZE(10 10)) -
 INDEX(NAME(NODLST1I.INDEX) -
          TRACKS(1))
```

2. Code the **INDEX** operand on the **DEFINE** command, or let it default. (See the preceding sample **DEFINE** command.) The data set must be indexed.
3. Code **KEYS** (2 0). A key length of 2 bytes and an offset of 0 bytes are required.
4. Code **RECORDSIZE** (10 10). The average record and the maximum record must each have a length of 10 bytes.
5. Make sure that the number of records in the file is equal to the number of major node and dynamic reconfiguration data set (DRDS) file activations that occur from the time z/OS Communications Server is started until it is halted. This includes major nodes that are reactivated. The primary allocation should be about 1.2 times the total number of major nodes and DRDS files in the network, and the secondary allocation should be about 0.2 times the total number.

You can use defaults for all other data characteristics.

Data sets containing information for NCP

This section describes some of the data sets that contain information for NCP. You might need to define these data sets for your communication controller.

NCP load library

The NCP load library contains the NCP and the resource resolution table (RRT) load modules.

To load NCP, create an NCP load module data set to allocate space. Cataloging the data set is optional. To activate the NCP, the NCP load library must also be available so that the RRT can be accessed.

Figure 1 shows the correlation between the DD statement for the NCP load module data set and the **NCP BUILD** definition statement.

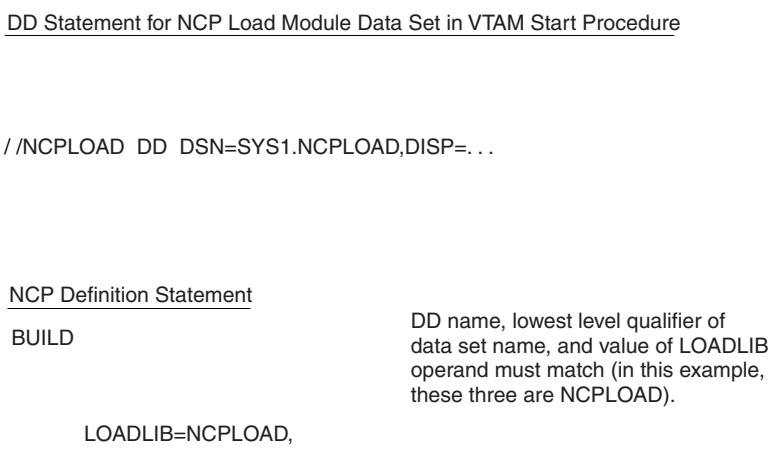


Figure 1. Correlation between DD statement and NCP definition statement

NCP load module data sets must be in an authorized program facility (APF) library. Since z/OS Communications Server must be loaded from an authorized library, the system verifies that all modules subsequently loaded by z/OS Communications Server be contained in authorized libraries. If the NCP load library is not APF authorized, an ABEND306 may occur when z/OS Communications Server attempts to load the NCP RRT during an NCP activation. An NCP load module data set can contain more than one NCP.

SYS1.SSPLIB

SYS1.SSPLIB contains the System Support Program (SSP) utilities used by NCP. SYS1.SSPLIB is a required partitioned data set and is added when NCP is installed. It must be in one of these places:

- SYS1.LINKLIB
- A concatenation of SYS1.LINKLIB (a library listed in the currently used LNKLSTxx parmlib member)
- A STEPLIB in the start procedure, to specify an authorized program facility (APF) library

NCP dump

The NCP dump data set receives the NCP dump output (one data set for each host z/OS Communications Server). To dump NCP, you need to allocate space for this data set. You can also catalog this data set. The name of the NCP dump data set is defined when NCP is coded.

This dump data set must accommodate a dump of the entire communication controller storage. The size of communication controller storage depends on the model number.

The DD statement defines the dump data set for the communication controller. The *ddname* must match the *ddname* on the DUMPDS operand of the PCCU definition statement for the associated NCP. z/OS Communications Server has no restrictions on the data set name.

z/OS Communications Server dump processing fails if the SSP modules that need to be loaded to process the dump are not accessible to z/OS Communications Server. See "SYS1.SSPLIB" on page 19 for information on SYS1.SSPLIB requirements.

For more information about the NCP dump data set, see the *NCP, SSP, and EP Diagnosis Guide*.

Loader channel I/O trace

The loader channel I/O trace data set (LDRIOTAB) receives communication controller channel information if a load of an NCP fails. The information collected includes channel control words, channel status words, and the first 20 bytes of any data associated with a **WRITE**, **WRITEIPL**, or **WRITEBRK** channel command.

The DD statement defines the trace data set for the SSP load utility. The *ddname* must be LDRIOTAB, but there are no restrictions on the data set name. The data requires only one track of DASD storage and should have a blocksize and logical record length of 121. The data set must be allocated before it is defined in the z/OS Communications Server start procedure.

Set the disposition of the data set as share, pass, and keep in the z/OS Communications Server start procedure.

See *NCP, SSP, and EP Trace Analysis Handbook* for more information about the loader channel I/O trace data set.

CSP and MOSS dump (IBM 3720, 3725, and 3745 only)

The communication scanner processor (CSP) and maintenance and operator subsystem (MOSS) dump data sets, which apply only to the IBM 3720, 3725, and 3745 Communication Controllers, are used for traces of the CSP and MOSS. To dump the CSP and MOSS microcode for problem determination, create one data set for the dump of each component. These data sets can be cataloged. The names of these data sets are defined to z/OS Communications Server in the start procedure.

The DD statement for each dump data set defines it for the NCP utility used to dump the communication controller. The *ddname* must match the *ddname* on the **CDUMPDS** (for a CSP dump) or **MDUMPDS** (for a MOSS dump) operand of the **PCCU** definition statement for the appropriate NCP. z/OS Communications Server has no restrictions on the data set name.

Chapter 2. Roadmap to functions

This topic includes a roadmap table to all of the functions and enhancements that were introduced in z/OS V1R12 Communications Server and z/OS V1R11 Communications Server.

The **Exploitation actions** column indicates whether tasks are required to either use the functional enhancement or to satisfy incompatibilities or dependencies.

Table 8. Roadmap to functions

Functional enhancement	Exploitation actions
Enhancements introduced in z/OS V1R12 Communications Server	
"Enhancements to IPv6 router advertisement" on page 25	Yes
"Configurable default address selection policy table" on page 26	Yes
"Socket API support for source address selection" on page 26	Yes
"Resolver support for IPv6 connections to DNS name servers" on page 27	Yes
"Performance improvements for sysplex distributor connection routing" on page 28	Yes
"Performance improvements for streaming bulk data" on page 29	Yes
"z/OS Communications Server in an ensemble" on page 31	Yes
"Extend sysplex distributor support for DataPower for IPv6" on page 32	Yes
"Improvements to AT-TLS performance" on page 33	No
"Sysplex distributor support for hot-standby server" on page 33	Yes
"Common storage reduction for TN3270E server" on page 34	Yes
"Performance improvements for fast local sockets" on page 34	No
"Improved resolver reaction to unresponsive DNS name servers" on page 34	No
"Sysplex autonomics monitoring TCP/IP abends" on page 35	No
"IKE version 2 support" on page 35	Yes
"IPSec support for certificate trust chains and certificate revocation lists" on page 37	Yes
"IPSec support for cryptographic currency" on page 38	Yes
"IPSec support for FIPS 140 cryptographic mode" on page 39	Yes
"Trusted TCP connections" on page 40	Yes
"Digital certificate access server (DCAS) MODIFY command for debug level" on page 41	Yes
"Enhancements to the TN3270E server" on page 41	Yes
"IBM Health Checker for z/OS OMPROUTE checks" on page 42	Yes
"Command to drop all connections for a server" on page 42	Yes
"Control joining the sysplex XCF group" on page 43	Yes
"Extension of the retry time limit for CSSMTP" on page 43	Yes
"Enterprise Extender connection health verification" on page 44	Yes
"Multipath control for Enterprise Extender" on page 45	Yes
"Improved recovery from RTP pipe stalls" on page 45	No
"Enhancements to topology database diagnostics" on page 45	Yes

Table 8. Roadmap to functions (continued)

Functional enhancement	Exploitation actions
"Performance improvement to TCP/IP callable NMI (EZBNMIFR) GetConnectionDetail request" on page 46	No
"Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics" on page 46	Yes
"SMF event records for sysplex events" on page 47	Yes
"Management data for CSSMTP" on page 47	Yes
"Data trace records for socket data flow start and end" on page 49	Yes
"Enhancements to the TN3270E server - session manager sends CV64" on page 49	Yes
"Operator command to query and display OSA information" on page 50	Yes
"Packet trace filtering for encapsulated packets" on page 50	Yes
"Verify Netstat message catalog synchronization" on page 51	Yes
"Enhancements to the TCP/IP storage display" on page 51	Yes
"Enhancements to SNMP manager API" on page 51	Yes
Enhancements introduced in z/OS V1R11 Communications Server	
"New SMTP client for sending Internet mail" on page 54	Yes
"FTP access to UNIX named pipes" on page 56	Yes
"FTP large-volume access" on page 61	Yes
"FTP passive mode enhancements" on page 61	Yes
"Customizable pre-logon banner for otelnetd" on page 63	Yes
"Remote execution server enhancements" on page 63	Yes
"TN3270 support of TSO logon reconnect" on page 64	No
"IPv6 stateless address autoconfiguration enhancements" on page 64	Yes
"New API to obtain IPv4 network interface MTU" on page 66	Yes
"RFC 5095 deprecation of IPv6 type 0 route header" on page 66	No
"CICS sockets enhancements" on page 67	No
"Improved responsiveness to storage shortage conditions" on page 67	Yes
"Disable moving DVIPA as source IP address" on page 68	No
"Support for enhanced WLM routing algorithms" on page 68	Yes
"accept_and_receive API enhancements" on page 69	No
"TCP/IP support for system z10 hardware instrumentation" on page 70	No
"TCP/IP pathlength improvements" on page 70	No
"TCP throughput improvements for high-latency networks" on page 71	Yes
"Virtual storage constraint relief" on page 71	Yes
"NSS private key and certificate services for XML appliances" on page 72	Yes
"Enterprise Extender IPSec performance improvements" on page 72	No
"Resolver DNS cache" on page 73	Yes
"Sysplex autonomics improvements for FRCA" on page 74	No
"QDIO routing accelerator" on page 74	Yes
"Sysplex distributor connection routing accelerator" on page 76	Yes
"Sysplex distributor optimization for multi-tier z/OS workloads" on page 76	No

Table 8. Roadmap to functions (continued)

Functional enhancement	Exploitation actions
"Sysplex distributor support for DataPower" on page 77	Yes
"OSA-Express3 optimized latency mode" on page 78	Yes
"IPSec enhancements" on page 79	No
"AT-TLS enhancements" on page 80	Yes
"Configuration Assistant enhancements" on page 81	Yes
"syslogd enhancements" on page 82	Yes
"syslogd browser and search facilities" on page 82	Yes
"Policy infrastructure management enhancements" on page 83	Yes
"MVS console support for select TCP/IP commands" on page 85	Yes
"IBM Health Checker for z/OS DNS server check" on page 85	Yes
"Display potential model application name" on page 86	Yes
"Include data space VIT with INOP dump" on page 86	Yes
"HPR performance enhancements" on page 87	Yes
"APPN topology database update enhancements" on page 90	Yes
"Provide ACF/TAP as part of z/OS Communications Server" on page 91	Yes
"IBM Health Checker for z/OS RFC 4301 compliance" on page 92	Yes
Network management enhancements - "Stack configuration data" on page 92	Yes
Network management enhancements - "Detailed CSM usage" on page 93	Yes
Network management enhancements - "OSA network traffic analyzer data" on page 94	Yes
Network management enhancements - "Sysplex networking data" on page 95	Yes
"Verbose Ping" on page 96	Yes
"QDIO enhancements for Workload Manager IO priority" on page 96	Yes
"QDIO support for OSA interface isolation" on page 97	Yes

Chapter 3. V1R12 new function summary

This information contains topics about every function or enhancement introduced in z/OS V1R12 Communications Server. The topics describe each function and present the following information, if applicable:

- Restrictions, dependencies, and coexistence considerations for the function
- A task table that identifies the actions necessary to use the function
- References to the documents that contain more detailed information

See Table 8 on page 21 for a complete list of the functional enhancements.

See *z/OS Migration* for information about how to migrate and maintain the functional behavior of previous releases.

See *z/OS Summary of Message and Interface Changes* for information about new and changed messages and interfaces.

Application integration, data consolidation, and standards

The following topics describe enhancements for application integration, data consolidation, and standards:

- "Enhancements to IPv6 router advertisement"
- "Configurable default address selection policy table" on page 26
- "Socket API support for source address selection" on page 26
- "Resolver support for IPv6 connections to DNS name servers" on page 27

Enhancements to IPv6 router advertisement

z/OS V1R12 Communications Server supports the enhancements to IPv6 router advertisement messages that are described in RFC 4191 and RFC 5175. The enhancements include:

- The ability to learn indirect prefix routes from IPv6 router advertisement messages
- The ability to associate preference values with default routes and indirect prefix routes that are learned from IPv6 router advertisement messages

This function is automatically enabled. Use the tasks in Table 9 to display IPv6 routes.

Table 9. Enhancements to IPV6 router advertisement

Task	Reference
Display all the IPv6 routes that were added as a result of information received in router advertisement messages by issuing the Netstat ROUTe/-r command with the RADV modifier.	• Netstat ROUTe/-r report in *z/OS Communications Server: IP System Administrator's Commands* • *z/OS Communications Server: IPv6 Network and Application Design Guide*
Display all the IPv6 routes that were added as a result of information received in router advertisement messages by issuing the TCPIPCS ROUTE command with the RADV parameter.	• TCPIPCS ROUTE in *z/OS Communications Server: IP Diagnosis Guide* • *z/OS Communications Server: IPv6 Network and Application Design Guide*

Configurable default address selection policy table

z/OS V1R12 Communications Server supports RFC 3484 by providing a configurable policy table for default address selection for IPv6. The source address selection algorithm and destination address selection algorithm support additional address selection rules with the configured or default policy table.

The SRCIP configuration statement can now indicate that the TCP/IP stack prefers public IPv6 addresses over temporary IPv6 addresses.

Using the configurable default address selection policy table

If you want to use the configurable default address selection policy table, perform the appropriate tasks in Table 10.

Table 10. Configurable default address selection policy table

Task	Reference
Configure the default address selection policy table using the DEFADDRTABLE TCP/IP profile block statement.	• DEFADDRTABLE statement in *z/OS Communications Server: IP Configuration Reference* • Default address selection policy table in *z/OS Communications Server: IPv6 Network and Application Design Guide*
Display the default address selection policy table by issuing the Netstat DEFADDRT/-l command.	DEFADDRT/-l report in *z/OS Communications Server: IP System Administrator's Commands*
Set TCP/IP stack preference to public or temporary IPv6 addresses for a specific job name by specifying JOBNAME *jobname* PUBLICADDRS or TEMPADDRS in the SRCIP TCP/IP profile block statement. This entry overrides any preference specified by the new source address selection API support that was added in this release.	SRCIP statement in *z/OS Communications Server: IP Configuration Reference*
Display the configured SRCIP entries by issuing the Netstat SRCIP/-J command.	Netstat SRCIP/-J report in *z/OS Communications Server: IP System Administrator's Commands*

Socket API support for source address selection

z/OS V1R12 Communications Server supports RFC 5014 by providing an IPv6 socket API for source address selection. This support implements sockets API extensions for the following languages:

- z/OS XL C/C++
- z/OS UNIX System Services (z/OS UNIX) callable services
- Language Environment® C/C++
- z/OS UNIX System Services Assembler Callable (BPX1* and BPX4*)
- REXX socket API EZASMI macro ASM
- CALL instruction API
- CICS C Sockets
- CICS EZASMI macro ASM
- CICS EZASOKET callable for ASM, PL/I, and Cobol

Restrictions:

- The IPV6_ADDR_PREFERENCES socket option defined in RFC 5014 is supported for TCP and UDP sockets, but not RAW sockets.

- The ancillary data object support for altering default source address selection that is described in Appendix A of RFC 5014 is not supported by z/OS V1R12 Communications Server.
- In a CINET environment with multiple stacks, CINET might not select the optimal stack for API calls because CINET is not aware of application address preferences or of the default address selection policy table that is in use on each stack.

Using the socket API support for source address selection

If you want to use the socket API support for source address selection, perform the appropriate tasks in Table 11.

Table 11. Socket API support for source address selection

Task	Reference
Use the socket API to specify whether your application prefers temporary or public addresses when TCP/IP selects an IPv6 source address for a TCP connection using the default address selection algorithms. If a JOBNAME *jobname* PUBLICADDRS or TEMPADDRS statement is specified in the SRCIP block statement, the API preference is ignored.	• SRCIP statement in *z/OS Communications Server: IP Configuration Reference* • RFC 5014 *IPv6 Socket API for Source Address Selection* • *z/OS UNIX System Services Programming: Assembler Callable Services Reference* • *z/OS XL C/C++ Run-Time Library Reference*
For an IPv6 connection, determine the source address preference by using the INET6_IS_SRCADDR function.	• RFC 5014 *IPv6 Socket API for Source Address Selection* • The following topics in *z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference*: – INET6_IS_SRCADDR for the macro for assembler instruction – INET6_IS_SRCADDR for the code CALL instruction • *z/OS XL C/C++ Run-Time Library Reference*

Resolver support for IPv6 connections to DNS name servers

z/OS V1R12 Communications Server allows the system resolver to send requests to the Domain Name System (DNS) name servers using IPv6 communication. You use the existing NSINTERADDR and NAMESERVER resolver configuration statements in the TCPIP.DATA data set to define the IPv6 address of the name server.

Restrictions: The res_state structure (nsaddr_list) contains only the IPv4 addresses coded on the NSINTERADDR or NAMESERVER statements. Applications that examine or update the nsaddr_list cannot manipulate the IPv6 addresses.

Using the resolver support for IPv6 connections to DNS name servers

If you want to use this function, perform the appropriate tasks in Table 12.

Table 12. Resolver support for IPv6 connections to DNS name servers

Task	Reference
Increase the MAXSOCKETS value on the BPXPRMxx AF_INET6 NETWORK statement, if necessary, to accommodate the usage of IPv6 sockets by the resolver for communication with IPv6 name servers.	Using IPv6 name servers in *z/OS Communications Server: IP Configuration Guide*

Table 12. Resolver support for IPv6 connections to DNS name servers (continued)

Task	Reference
Define the IPv6 addresses to be used to communicate with a DNS name server using either the NSINTERADDR or the NAMESERVER resolver configuration statement in the TCPIP.DATA file.	• NSINTERADDR statement and NAMESERVER statement in *z/OS Communications Server: IP Configuration Reference* • Using IPv6 name servers in *z/OS Communications Server: IP Configuration Guide*
Verify the list of name servers being used by an application that is using the updated TCPIP.DATA file by performing the following tasks: 1. Direct the trace resolver output to your workstation or to a file or data set where it can be examined. 2. Request the Netstat Up/-u report. Requesting this report causes Netstat to issue a res_init API call, which generates information about the resolver parameters being used by this application. 3. Examine the trace resolver output and use the name server information to determine the list of name servers being used. Any IPv6 addresses included in the list of name servers is displayed in the trace resolver output.	• Verifying TCPIP.DATA statement values in the native MVS environment and Verifying TCPIP.DATA statement values in the z/OS UNIX environment in *z/OS Communications Server: IP Configuration Guide* • Netstat Up/-u report in *z/OS Communications Server: IP System Administrator's Commands* • Diagnosing resolver problems in *z/OS Communications Server: IP Diagnosis Guide*

Scalability, performance, constraint relief, and accelerators

z/OS V1R12 Communications Server includes the following enhancements to scalability, performance, constraint relief, and accelerators:

- "Performance improvements for sysplex distributor connection routing"
- "Performance improvements for streaming bulk data" on page 29
- "z/OS Communications Server in an ensemble" on page 31
- "Extend sysplex distributor support for DataPower for IPv6" on page 32
- "Improvements to AT-TLS performance" on page 33
- "Sysplex distributor support for hot-standby server" on page 33
- "Common storage reduction for TN3270E server" on page 34
- "Performance improvements for fast local sockets" on page 34
- "Improved resolver reaction to unresponsive DNS name servers" on page 34
- "Sysplex autonomics monitoring TCP/IP abends" on page 35

Performance improvements for sysplex distributor connection routing

In z/OS V1R12 Communications Server, processing for OSA-Express in QDIO mode supports inbound workload queueing. Inbound workload queueing uses multiple input queues for each QDIO data device (subchannel device) to improve TCP/IP stack scalability and general network optimization. Implement the performance improvements for sysplex distributor connection routing by enabling inbound workload queueing to process sysplex distributor traffic concurrently with other types of inbound QDIO traffic. When you enable these improvements for a QDIO interface, inbound sysplex distributor traffic is processed on an ancillary input queue (AIQ). All other inbound traffic is processed on the primary input queue or on an ancillary input queue for streaming bulk data.

Restrictions: This function is not supported when z/OS V1R12 Communications Server is running as a z/OS guest on z/VM® that is using simulated (virtual) devices such as Virtual Switch (VSWITCH) or guest LAN.

Incompatibilities: This function is not supported for IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.

Dependencies:

- This function is limited to OSA-Express3 Ethernet features that are in QDIO mode and that are running on a minimum of an IBM System z10. See the 2097DEVICE and the 2098DEVICE Preventive Service Planning (PSP) buckets for further information.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

Coexistence consideration: Using this function also enables the performance improvements for streaming bulk data; see "Performance improvements for streaming bulk data."

Using the performance improvements for sysplex distributor connection routing

If you want to use this function, perform the appropriate tasks in Table 13.

Table 13. Performance improvements for sysplex distributor connection routing

Task	Reference
Enable inbound workload queueing for a specific QDIO interface by specifying INBPERF DYNAMIC WORKLOADQ on the IPAQENET or IPAQENET6 INTERFACE statement (if necessary). For IPv4 QDIO interfaces that are defined by using the DEVICE, LINK, and HOME statements, you must first convert the statement definitions to use an IPAQENET INTERFACE statement.	• INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces statements in *z/OS Communications Server: IP Configuration Reference* • Steps to convert from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement in *z/OS Communications Server: IP Configuration Guide*
Display whether inbound workload queueing is in effect for the QDIO interface by issuing the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d report in *z/OS Communications Server: IP System Administrator's Commands*
Display whether inbound workload queueing is in effect for the QDIO interface (and display the relationship between workload queueing functions and queue IDs for that interface) by issuing the DISPLAY NET,ID=trle command or the DISPLAY NET,TRL,TRLE=trle command.	DISPLAY ID command and DISPLAY TRL command in *z/OS Communications Server: SNA Operation*
Monitor whether inbound traffic is using inbound workload queueing by initiating VTAM tuning statistics for the QDIO interface.	MODIFY TNSTAT command in *z/OS Communications Server: SNA Operation*
Determine whether specific IP traffic is using QDIO inbound workload queueing from a packet trace or OSAENTA trace.	Formatting packet traces using IPCS in *z/OS Communications Server: IP Diagnosis Guide*

Performance improvements for streaming bulk data

In z/OS V1R12 Communications Server, processing for OSA-Express in QDIO mode supports inbound workload queueing. Inbound workload queueing uses multiple input queues for each QDIO data device (subchannel device) to improve

TCP/IP stack scalability and general network optimization. Implement the performance improvements for streaming bulk data by enabling inbound workload queueing to process streaming bulk data traffic concurrently with other types of inbound QDIO traffic. When you enable these improvements for a QDIO interface, inbound traffic for connections that exhibit streaming bulk data behavior is processed on an ancillary input queue (AIQ). All other inbound traffic is processed on the primary input queue or on an ancillary input queue for sysplex distributor connection routing.

Restrictions: This function is not supported when z/OS V1R12 Communications Server is running as a z/OS guest on z/VM that is using simulated (virtual) devices such as Virtual Switch (VSWITCH) or guest LAN.

Incompatibilities: This function is not supported for IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.

Dependencies:

- This function is limited to OSA-Express3 Ethernet features that are in QDIO mode and that are running on a minimum of an IBM System z10. See the 2097DEVICE and the 2098DEVICE Preventive Service Planning (PSP) buckets for further information.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

Coexistence consideration: Using this function also enables the performance improvements for sysplex distributor connection routing; see "Performance improvements for sysplex distributor connection routing" on page 28.

Using the performance improvements for streaming bulk data

If you want to use this function, perform the appropriate tasks in Table 14.

Table 14. Performance improvements for streaming bulk data

Task	Reference
Enable inbound workload queueing for a specific QDIO interface by specifying INBPERF DYNAMIC WORKLOADQ on the IPAQENET or IPAQENET6 INTERFACE statement (if necessary). For IPv4 QDIO interfaces that are defined by using the DEVICE, LINK, and HOME statements, you must first convert the statement definitions to use an IPAQENET INTERFACE statement.	• INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces statements in *z/OS Communications Server: IP Configuration Reference* • Steps to convert from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement in *z/OS Communications Server: IP Configuration Guide*
Display whether inbound workload queueing is in effect for the QDIO interface by issuing the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d report in *z/OS Communications Server: IP System Administrator's Commands*
Display whether inbound workload queueing is in effect for the QDIO interface (and display the relationship between workload queueing functions and queue IDs for that interface) by issuing the DISPLAY NET,ID=trle command or the DISPLAY NET,TRL,TRLE=trle command.	DISPLAY ID command and DISPLAY TRL command in *z/OS Communications Server: SNA Operation*
Monitor whether inbound traffic is using inbound workload queueing by initiating VTAM tuning statistics for the QDIO interface.	MODIFY TNSTAT command in *z/OS Communications Server: SNA Operation*

Table 14. Performance improvements for streaming bulk data (continued)

Task	Reference
Determine whether a QDIO inbound workload queueing bulk data queue is being used for a TCP connection. Perform one of the following actions: • Invoke the Netstat ALL/-A command. • Update your network management application to use the information returned by the GetConnectionDetail callable NMI.	• Netstat ALL/-A report in *z/OS Communications Server: IP System Administrator's Commands* • GetConnectionDetail request (an EZBNMIFR request) in *z/OS Communications Server: IP Programmer's Guide and Reference*
Display the total number of TCP segments processed on all bulk data queues by invoking the Netstat STATS/-S command or updating your network management application to invoke the GetGlobalStats callable NMI.	Netstat ALL/-A report in *z/OS Communications Server: IP System Administrator's Commands*
Determine whether specific IP traffic is using QDIO inbound workload queueing from a packet trace or OSAENTA trace.	Formatting packet traces using IPCS in *z/OS Communications Server: IP Diagnosis Guide*

z/OS Communications Server in an ensemble

The IBM zEnterprise 196 (z196) offers communications access to two new internal networks through OSA-Express3 adapters that are configured with an appropriate channel path ID (CHPID) type. The following list describes the two new internal networks:

- The intranode management network - It provides connectivity between network management applications within the z196 node and it can be accessed through 1000BASE-T Ethernet OSA-Express3 adapters that are configured with a CHPID type of OSM.
- The intraensemble data network - It provides access to other images that are connected to the intraensemble data network and to applications and appliances that are running in an IBM zEnterprise BladeCenter® Extension (zBX). This internal network can be accessed through 10 gigabit OSA-Express3 adapters that are configured with a CHPID type of OSX.

z/OS V1R12 Communications Server adds support for OSA-Express3 adapters that are configured with the new OSM and OSX CHPID types, thus allowing TCP/IP connectivity to the two new internal networks. This support eases the burden of configuration for these new OSA-Express3 CHPID types because it enables TCP/IP to dynamically find and activate up to two OSA-Express3 adapters that are connected to the intranode management network. The support requires minimal configuration for OSA-Express3 adapters that are connected to the intraensemble data network.

Restrictions:

- Access to the intranode management network is restricted to authorized management applications, and is only available through Port 0 of any OSA-Express3 CHPID configured with type OSM. Port 1 is not available for these communications.
- Connectivity to the intranode management network is restricted to stacks that are enabled for IPv6.
- Connectivity to the intranode management network and to the intraensemble data network is allowed only when the central processor complex (CPC) is a member of an ensemble.

Dependencies:

- This function is limited to OSA-Express3 Ethernet features configured with CHPID types of OSX and OSM running on a z196. See the 2817DEVICE Preventive Service Planning (PSP) bucket for more information.
- This function is dependent upon the z/OS LPAR participating in an ensemble. See *zEnterprise System Ensemble Planning and Configuring Guide* for more information.

Using z/OS Communications Server in an ensemble

If you want to use this function, perform the appropriate tasks in Table 15.

Table 15. z/OS Communications Server in an ensemble

Task	Reference
Allow z/OS Communications Server to have connectivity to the intranode management network and to the intraensemble data network by specifying ENSEMBLE=YES as a VTAM start option.	ENSEMBLE start option in *z/OS Communications Server: SNA Resource Definition Reference*
Allow a host management application to have access to the intranode management network by defining the SERVAUTH profile EZB.OSM.sysname.tcpname and by permitting the host management application to have access to that resource.	TCP/IP in an ensemble in *z/OS Communications Server: IP Configuration Guide*
For any TCP/IP stack needing access to the intraensemble data network, define INTERFACE statements as required for each OSA-Express3 CHPID that is configured with a CHPID type of OSX through which access is needed. Define INTERFACE statements for each IP version to be used (IPv4, IPv6, or both). If you require access over multiple VLANs, define an INTERFACE statement for each VLAN that is accessed over the OSA-Express3 interface.	• INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces statements in *z/OS Communications Server: IP Configuration Reference* • TCP/IP in an ensemble in *z/OS Communications Server: IP Configuration Guide*
Display information for OSA-Express3 interfaces that are providing connectivity to the internal networks by issuing the Netstat/DEvlinks/-d command, DISPLAY NET,ID=trle, or the DISPLAY NET,TRL,TRLE= command.	• Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands* • DISPLAY ID command and DISPLAY TRL command in *z/OS Communications Server: SNA Operation*
If IPSec is configured and you want a security class for IP filtering for intranode management network interfaces, specify OSMSECCLASS on the IPCONFIG6 statement.	• IPCONFIG6 statement in *z/OS Communications Server: IP Configuration Reference* • TCP/IP in an ensemble in *z/OS Communications Server: IP Configuration Guide*
Display the security class for IP filtering for intranode management network interfaces.	Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*

Extend sysplex distributor support for DataPower for IPv6

z/OS V1R12 Communications Server introduces sysplex distribution of IPv6 connections to non-z/OS targets, which is similar to the sysplex distribution of IPv4 connections to non-z/OS targets that was introduced in z/OS V1R11 Communications Server (see "Sysplex distributor support for DataPower" on page 77).

An IBM WebSphere® DataPower® appliance is currently the only non-z/OS target that supports sysplex distributor load balancing. DataPower appliances are often

used as a front-end processing tier for z/OS applications, which provides more efficient handling of Web services for a second tier of z/OS applications. When the DataPower tier completes a request, DataPower can route the request to a tier 2 sysplex distributor, which can load balance the request to the second tier of z/OS applications.

Restriction: All TCP/IP stacks that participate in an IPv6 sysplex distribution to a DataPower appliance must be V1R12 or later.

Coexistence requirements: An IBM WebSphere DataPower Integration Appliance V3.8.1 or later is required to use this function.

Extending sysplex distributor support for DataPower for IPv6

If you want to use this function, perform the task in Table 16.

Table 16. Extend sysplex distributor support for DataPower for IPv6

Task	Reference
Use sysplex distribution with DataPower in an IPv6 environment.	sysplex distribution with DataPower in *z/OS Communications Server: IP Configuration Guide*

Improvements to AT-TLS performance

In z/OS V1R12 Communications Server, the Application Transparent - Transport Layer Security (AT-TLS) processing provides reduced CPU usage when encrypting and decrypting application data. This function is automatically enabled.

Sysplex distributor support for hot-standby server

z/OS V1R12 Communications Server introduces sysplex distributor support for hot-standby server through the use of a new distribution method, HotStandby. You configure a preferred server and one or more hot-standby servers. The preferred server that has an active listener receives all new incoming connection requests, and the hot-standby servers act as backup servers in case the designated preferred server become unavailable. You can rank the hot-standby servers to control which hot-standby server becomes the active server. You can also control whether the sysplex distributor automatically switches back to using the preferred server if it again becomes available, and whether the distributor automatically switches servers if the active target is not healthy.

Restriction: The sysplex distributor must be V1R12 or later and the TCP/IP target stacks must be V1R10 or later.

Using the sysplex distributor support for hot-standby server

If you want to use this function, perform the appropriate tasks in Table 17.

Table 17. Sysplex distributor support for hot-standby server

Task	Reference
Configure the hot-standby function by specifying the following parameters and options on the VIPADISTRIBUTE statement: • The HOTSTANDBY option on the DISTMETHOD parameter • Optionally, the NOAUTOSWITCHBACK and NOHEALTHSWITCH options for HOTSTANDBY on the DISTMETHOD parameter • The PREFERRED or BACKUP option on the DESTIP parameter	• VIPADISTRIBUTE statement in *z/OS Communications Server: IP Configuration Reference* • sysplex distributor and Steps for configuring hot standby distribution in *z/OS Communications Server: IP Configuration Guide*

Common storage reduction for TN3270E server

In z/OS V1R12 Communications Server, the TN3270E Telnet server provides access method control block (ACB) sharing for Telnet logical units (LUs) as a way to reduce extended common storage area (ECSA) usage. Before z/OS V1R12 Communications Server, every Telnet LU name opened its own ACB to VTAM. You can code a new SHAREACB statement to enable multiple Telnet LUs to share a single ACB, which reduces the overall amount of ECSA (and Telnet private) storage allocated to support Telnet sessions.

Telnet LU ACB sharing can benefit your installation if you currently run many connections to a given Telnet server.

Using common storage reduction for TN3270E server

If you want to use this function, perform the appropriate tasks in Table 18.

Table 18. Common storage reduction for TN3270E server

Task	Reference
Specify the SHAREACB statement in the TELNETGLOBALS section of the Telnet profile to enable ACB sharing.	• Reducing demand for ECSA storage in *z/OS Communications Server: IP Configuration Guide* • SHAREACB statement in *z/OS Communications Server: IP Configuration Reference*
Replace any predefined (static) APPL definition statements that are used to represent Telnet LUs with corresponding model application program definition statements.	Reducing demand for ECSA storage in *z/OS Communications Server: IP Configuration Guide*
Verify that ACB sharing is correctly implemented by issuing the DISPLAY Telnet PROFILE command.	DISPLAY Telnet PROFILE command in *z/OS Communications Server: IP System Administrator's Commands*

Performance improvements for fast local sockets

z/OS V1R12 Communications Server enhances the performance of fast local sockets for TCP connections. There are no tasks to use this function; it is automatically enabled.

Improved resolver reaction to unresponsive DNS name servers

z/OS V1R12 Communications Server provides notification to the operator console when a Domain Name System (DNS) name server does not respond to a certain percentage of resolver queries that are sent to the name server during a sliding 5-minute interval. In addition to the notification, statistics regarding the number of queries attempted and the number of queries which received no response are displayed for each currently unresponsive name server at 5-minute intervals.

The default value for the TCPIP.DATA RESOLVERTIMEOUT configuration statement, which controls the timeout value for UDP requests sent to a name server, is now 5 seconds instead of 30 seconds.

Using the improved resolver reaction to unresponsive DNS name servers

The system default is 25% of resolver queries sent to the name server. There are no tasks to enable this function; it is automatically enabled. You can optionally perform the task in Table 19 on page 35.

Table 19. Improved resolver reaction to unresponsive DNS name servers

Task	Reference
Change the threshold percentage that must be exceeded for a name server to be declared unresponsive by using the UNRESPONSIVETHRESHOLD configuration statement in the resolver setup file. Set the new percentage threshold by performing one of the following tasks: • If the resolver is active, issue the MODIFY *resolver*,REFRESH,SETUP=*setup_file_name* command. • If the resolver is not active, start it and ensure that the correct resolver setup file is used during activation.	• UNRESPONSIVETHRESHOLD in *z/OS Communications Server: IP Configuration Reference* • MODIFY command: Resolver address space in *z/OS Communications Server: IP System Administrator's Commands* • Monitoring the responsiveness of Domain Name System name servers in *z/OS Communications Server: IP Configuration Guide*

Sysplex autonomics monitoring TCP/IP abends

z/OS V1R12 Communications Server improves sysplex problem detection and recovery so that the sysplex detects when the TCP/IP stack has ended abnormally five times in less than a minute.

There are no tasks to enable this function; it is automatically enabled. For more information about sysplex autonomics, see Sysplex problem detection and recovery in *z/OS Communications Server: IP Configuration Guide*.

Security

z/OS V1R12 Communications Server includes enhancements to security in the following areas:

- "IKE version 2 support"
- "IPSec support for certificate trust chains and certificate revocation lists" on page 37
- "IPSec support for cryptographic currency" on page 38
- "IPSec support for FIPS 140 cryptographic mode" on page 39
- "Trusted TCP connections" on page 40
- "Digital certificate access server (DCAS) MODIFY command for debug level" on page 41

IKE version 2 support

Internet Key Exchange version 2 (IKEv2) is the second version of the Internet Key Exchange (IKE) protocol, which is used by peer nodes to perform mutual authentication and to establish and maintain Security Associations (SAs). In z/OS V1R12 Communications Server, the IKE daemon (IKED) supports IKEv2, in addition to supporting IKEv1. The z/OS V1R12 Communications Server IKEv2 support includes the following items:

- IPv4 and IPv6 support
- A new identity type, KeyID.

  Note: KeyID is also supported for IKEv1.
- Authentication using pre-shared keys or digital certificates; certificates can use RSA or elliptic curve keys
- Re-keying and re-authentication of IKE SAs and child SAs
- Hash and URL encoding of certificates and certificate bundles

Restrictions:

- z/OS Communications Server IKEv2 cannot be used to negotiate Sysplex-Wide Security Associations (SWSA).
- z/OS Communications Server IKEv2 does not support Network Address Translation (NAT) traversal.

Incompatibilities: IKEv2 must be supported by both peer nodes in order for the SA to be negotiated using IKEv2 flows. You can configure z/OS Communications Server to continue to use IKEv1 with peers that do not support IKEv2.

Dependencies: To activate IKEv2 SAs using certificate-based authentication methods, you must configure IKED as a network security services (NSS) client that is authorized for certificate services, and its NSS server must be at the V1R12 level. If IKED does not have an NSS server that is at the latest level providing certificate services, it can activate IKEv2 SAs only if pre-shared key authentication is used.

Enabling IKE version 2 support

z/OS V1R12 Communications Server is always enabled for IKEv2 as a responder. If you want to enable the IKE daemon to initiate IPsec SAs using IKEv2 protocols, perform the task in Table 20.

Table 20. Enabling IKE version 2 support

Task	Reference
Specify the value of IKEv2 on the HowToInitiate parameter on the KeyExchangePolicy statement, the KeyExchangeAction statement, or both of those statements in the IPsec policy. If you are using the IBM Configuration Assistant for z/OS Communications Server, set the default initiator mode in the IPSec perspective stack settings. You can modify the default initiator mode for each connectivity rule in the advanced settings for the rule. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis.	• KeyExchangePolicy statement and KeyExchangeAction statement in *z/OS Communications Server: IP Configuration Reference* • IBM Configuration Assistant for z/OS Communications Server online helps

Using hash and URL encoding of certificates and certificate bundles

If you want to use hash and URL encoding of certificates and certificate bundles, perform the appropriate tasks in Table 21.

Table 21. Using hash and URL encoding of certificates and certificate bundles

Task	Reference
If you want to use hash and URL encoding of certificate bundles, create certificate bundles by defining an X.509 bundle configuration file, issuing the certbundle command, and moving the bundle file to an HTTP server.	Creating certificate bundles in *z/OS Communications Server: IP Configuration Guide*

Table 21. Using hash and URL encoding of certificates and certificate bundles (continued)

Task	Reference
Enable local HTTP certificate usage by the NSS server by specifying the CertificateURL parameter or the CertificateBundleURL parameter in the NSS server configuration file. When using the IBM Configuration Assistant for z/OS Communications Server, set these values from the NSS perspective in the advanced server settings for the z/OS image. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis.	• Enabling the network security services daemon to use the hash and URL certificate encoding types in *z/OS Communications Server: IP Configuration Guide* • IBM Configuration Assistant for z/OS Communications Server online helps
Enable HTTP certificate retrieval in IKED by specifying the value Allow or Tolerate on the CertificateURLLookupPreference on the KeyExchangePolicy or KeyExchangeAction statements. If you are using the IBM Configuration Assistant for z/OS Communications Server, set the default certificate URL lookup preference in the advanced stack settings of the IPSec perspective. You can modify the default mode for each connectivity rule in the advanced settings for the rule. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis.	• KeyExchangePolicy statement and KeyExchangeAction statement in *z/OS Communications Server: IP Configuration Reference* • IBM Configuration Assistant for z/OS Communications Server online helps

IPSec support for certificate trust chains and certificate revocation lists

z/OS V1R12 Communications Server introduces the following enhancements to the network security services (NSS) processing of IPSec certificate trust chains and certificate revocation lists:

- All the certificate authorities in the trust chain are considered when NSS is creating or verifying a signature for certificate authorities that are in the key ring.
- Certificate revocation information is used when available when NSS is verifying a certificate.

The z/OS Internet Key Exchange daemon (IKED) uses these new NSS daemon (NSSD) functions when a stack is configured as a network security client.

Restriction: Certificate trust chains and certificate revocation checking is applicable only to IKEv1 and IKEv2 configurations that use NSS certificate services.

Using IPSec support for certificate trust chains and certificate revocation lists

If you want to use the IPSec support for certificate trust chains and certificate revocation lists, perform the appropriate tasks in Table 22 on page 38.

Table 22. IPSec support for certificate trust chains and certificate revocation lists

Task	Reference
Configure NSS by using the IBM Configuration Assistant for z/OS Communications Server. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis. Describe the server, create the nssd.conf file, and distribute the nssd.conf file to the server system. Alternatively, you can create the nssd.conf file manually by using a text editor.	• Preparing to provide network security services in *z/OS Communications Server: IP Configuration Guide* • IBM Configuration Assistant for z/OS Communications Server online helps
Configure IPSec policy for NSS clients by using the IBM Configuration Assistant for z/OS Communications Server to define policy and distribute to client systems. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis. Alternatively, you can create the IPSec policy files manually using a text editor.	• IP security and Policy-based networking in *z/OS Communications Server: IP Configuration Guide* • IBM Configuration Assistant for z/OS Communications Server online helps

IPSec support for cryptographic currency

z/OS V1R12 Communications Server introduces the following enhancements to IPSec and IKE support for cryptographic currency:

- Support for the Advanced Encryption Standard (AES) algorithm in Cipher Block Chaining (CBC) mode for IP security. In addition to the previously existing support of AES with a 128-bit key length, z/OS V1R12 Communications Server supports AES with a 256-bit key length in CBC mode. Use the longer key length for highly sensitive data.
- Support for the AES algorithm in Galois Counter Mode (GCM) and in Galois Message Authentication Code (GMAC) mode for IP security. AES in GCM mode provides both confidentiality and data origin authentication. AES-GCM is an efficient algorithm for high-speed packet networks. AES in GMAC mode provides data origin authentication but does not provide confidentiality. Use AES-GMAC when confidentiality is not needed. AES-GMAC, like AES-GCM, is also an efficient algorithm for high-speed packet networks. z/OS V1R12 Communications Server supports both 128-bit and 256-bit key lengths for these algorithms.
- Support for the use of Hashed Message Authentication Mode (HMAC) in conjunction with the SHA2-256, SHA2-384, and SHA2-512 algorithms. You can use these algorithms as the basis for data origin authentication and integrity verification. The new algorithms, HMAC-SHA2-256-128, HMAC-SHA2-384-192, and HMAC-SHA2-512-256, ensure that the data is authentic and has not been modified in transit. Versions of these algorithms that are not truncated are available as pseudorandom functions (PRFs). These algorithms are called PRF-HMAC-SHA2-256, PRF-HMAC-SHA2-384, and PRF-HMAC-SHA2-512.
- Support for an authentication algorithm, AES128-XCBC-96, that ensures the data is authentic and not modified in transit.
- Support for elliptic curve digital signature algorithm (ECDSA) authentication

Restrictions:

- AES-GCM encryption is subject to export restrictions and might not be available in your country.
- Support for ECDSA is limited to IKEv2 configurations that use NSS certificate services.

Using IPSec support for cryptographic currency

If you want to use IPSec and IKE support for cryptographic currency, perform the appropriate tasks in Table 23.

Table 23. IPSec support for cryptographic currency

Task	Reference
Enable the Integrated Cryptographic Services Facility (ICSF) by configuring and starting it.	*z/OS Cryptographic Services ICSF Administrator's Guide*
Enable ECDSA authentication in IKED by specifying ECDSA-256, ECDSA-384 or ECDSA-521 on the HowToAuthMe parameter of the KeyExchangeAction statement in the Policy Agent IPSec configuration file. If you are using the IBM Configuration Assistant for z/OS Communications Server, set the IKEv2 authentication method for each connectivity rule in the additional IKEv2 options of the remote security endpoint panel. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis.	• KeyExchangeAction statement in *z/OS Communications Server: IP Configuration Reference* • IBM Configuration Assistant for z/OS Communications Server online helps
Configure new encryption and authentication algorithms. Configure relevant policy for IP security. If you are using the IBM Configuration Assistant for z/OS Communications Server, you will see the new encryption and authentication algorithms as choices for existing input fields. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis.	• See the following topics in *z/OS Communications Server: IP Configuration Reference*: – KeyExchangeAction statement – KeyExchangeOffer statement – IpDynVpnAction – IpDataOffer statement • IBM Configuration Assistant for z/OS Communications Server online helps

IPSec support for FIPS 140 cryptographic mode

z/OS V1R12 Communications Server supports Federal Information Processing Standard (FIPS) 140 security requirements for cryptographic modules for IP security. This standard is useful to organizations that use cryptographic-based security systems to protect sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information that is protected by the module. FIPS 140 dictates security requirements that should be satisfied by a cryptographic module to obtain higher degrees of assurance about the integrity of the module. FIPS 140 provides four increasing, qualitative levels of security that are intended to cover a wide range of potential applications and environments. z/OS V1R12 Communications Server support is for security level 1.

Restrictions:

- Diffe-Hellman Groups 1, 2, and 5 are not supported when FIPS 140 mode is configured.
- The DES encryption algorithm and the HMAC-MD5, HMAC-MD5-96, AES128-XCBC, or AES128-XCBC-96 algorithms for authentication or pseudo-random function are not supported when FIPS 140 mode is configured.
- When FIPS 140 mode is configured, tunnels that are using the AES-GCM combined-mode encryption and authentication algorithm or tunnels that are using the AES-GMAC authentication algorithm may not be used to distribute traffic for sysplex-wide security associations (SWSA). These tunnels can be

renegotiated if a DVIPA moves; however, connections to a MOVING DVIPA cannot use these tunnels. Clients connected to a MOVING DVIPA must reconnect in order to use the renegotiated tunnels.

- Certificates for RSA signature authentication that have key lengths less than 1024 bits are not supported for FIPS 140 mode.
- The use of pre-shared keys for authentication, when the keys are shorter than half the key length of the chosen authentication algorithm or pseudo-random function, are not supported for FIPS 140 mode.

Dependency: Integrated Cryptographic Service Facility (ICSF) must be active and configured in FIPS 140 mode before you can use the FIPS 140 support.

Using the IPSec support for FIPS 140 cryptographic mode

If you want to use the IPSec support for FIPS 140 cryptographic mode, perform the appropriate tasks in Table 24.

Table 24. IPSec support for FIPS 140 cryptographic mode

Task	Reference
Configure and enable FIPS 140 mode for IP security.	FIPS 140 and IP security in *z/OS Communications Server: IP Configuration Guide*
If FIPS 140 mode is enabled, configure ICSF and System SSL for FIPS 140 support.	• *z/OS Cryptographic Services ICSF Administrator's Guide* • *z/OS Cryptographic Services System SSL Programming*

Trusted TCP connections

z/OS V1R12 Communications Server introduces trusted TCP connections, which enable a sockets program to retrieve sysplex-specific connection routing information and partner security credentials for a socket that is connected. You can retrieve partner security credentials if both endpoints of a TCP connection reside in the same z/OS image, z/OS sysplex, or z/OS subplex, and the endpoints are in the same security domain. In such a topology, partner programs can use trusted connections to authenticate each other as an alternative to using an SSL/TLS connection with digital certificates for client and server authentication.

Restriction: Trusted TCP connections are not supported by the following z/OS Communications Server APIs:

- TCP C socket API
- X/Open Transport Interface (XTI)
- Pascal API

Using trusted TCP connections

If you want to use this function, perform the appropriate tasks in Table 25.

Table 25. Trusted TCP connections

Task	Reference
Enable an application to retrieve sysplex-specific connection routing information over a TCP socket connection.	• Sysplex-specific connection routing information and Steps for retrieving sysplex-specific connection routing information in *z/OS Communications Server: IP Programmer's Guide and Reference*

Table 25. Trusted TCP connections (continued)

Task	Reference
Enable applications in a sysplex to exchange security information over a TCP sockets connection by using the SIOCGPARTNERINFO ioctl and optionally the SIOCSPARTNERINFO ioctl to establish a trusted TCP connection between the applications.	• Partner security credentials and Steps for retrieving partner security credentials in *z/OS Communications Server: IP Programmer's Guide and Reference*
Display whether security credentials between partners were retrieved to create a trusted TCP connection.	• TCP trusted connection flag (TcpTrustedPartner) in the Netstat ALL/-A report in *z/OS Communications Server: IP System Administrator's Commands*
Modify TCP/IP network management interface (NMI) applications to use associated trusted TCP connections data.	• GetConnectionDetail request (an EZBNMIFR request) in *z/OS Communications Server: IP Programmer's Guide and Reference*
Develop a Java™ application to retrieve connection routing information and partner security credentials using the API for Java for the trusted TCP connections.	See the Javadoc information in the EZBTrustedPartnerdoc.jar file, which is installed in the directory /usr/include/java_classes (download the jar file to a workstation, unpack it, and read it in a Web browser).

Digital certificate access server (DCAS) MODIFY command for debug level

z/OS V1R12 Communications Server enhances the digital certificate access server (DCAS) so that you can modify the debug level without restarting the application.

Using the DCAS MODIFY command for debug level

If you want to use the DCAS MODIFY command for debug level, perform the task in Table 26.

Table 26. Digital certificate access server (DCAS) MODIFY command for debug level

Task	Reference
Modify the DCAS debug level without restarting the application.	MODIFY command--DCAS in *z/OS Communications Server: IP System Administrator's Commands*

Simplification and consumability

z/OS V1R12 Communications Server includes enhancements to simplification and consumability in the following areas:

- "Enhancements to the TN3270E server"
- "IBM Health Checker for z/OS OMPROUTE checks" on page 42
- "Command to drop all connections for a server" on page 42
- "Control joining the sysplex XCF group" on page 43
- "Extension of the retry time limit for CSSMTP" on page 43

Enhancements to the TN3270E server

In z/OS V1R12 Communications Server, the TN3270E Telnet server is enhanced to:

- Specify the jobname of the Telnet server issuing a Telnet message.
- Automatically shut down when an OMVS,SHUTDOWN command is issued.
- Pass the connection type (basic or secure) to the application on the CINIT using flags in the CV64 control vector.

Using the enhancements to the TN3270E server

If you want to use the CV64 security information passed to your application, perform the task in Table 27.

Table 27. Enhancements to the TN3270E server

Task	Reference
Modify your application to read the new flags on the CINIT CV64.	Connection information passed on the CINIT Control Vector 64 (CV64) in *z/OS Communications Server: IP Configuration Guide*

IBM Health Checker for z/OS OMPROUTE checks

The z/OS Health Checker for z/OS adds two new checks in z/OS V1R12 Communications Server; one check is for IPv4 routing and one check is for IPv6 routing. The checks determine whether the total number of indirect routes in the TCP/IP stack routing table exceeds a maximum threshold (the default value is 2000 for indirect routes). When this threshold is exceeded, OMPROUTE and the TCP/IP stack can potentially experience high CPU consumption from routing changes. A large routing table is considered to be inefficient in network design and operation.

Two new maximum threshold parameters are available that override the default values for the total number of IPv4 and IPv6 indirect routes in a TCP/IP stack routing table before warning messages are issued.

Dependencies: z/OS Health Checker for z/OS must be active before you can use this function.

Using the IBM Health Checker for z/OS OMPROUTE checks

If you want to use the IBM Health Checker for z/OS OMPROUTE checks, perform the task in Table 28.

Table 28. IBM Health Checker for z/OS OMPROUTE checks

Task	Reference
Add health checks and specify parameters for the maximum thresholds that relate to the total number of indirect routes in the IPv4 and IPv6 routing tables of the TCP/IP stack.	See the following topics in *IBM Health Checker for z/OS: User's Guide*: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

Command to drop all connections for a server

In z/OS V1R12 Communications Server, you can use the VARY TCPIP,,DROP command to drop all established TCP connections for servers that match the specified filter parameters. When you issue this command, all established TCP connections are dropped for each server that is found to match the specified filter parameters. You can filter by port, jobname, or server ASID.

Restriction: If multiple servers match the filter criteria but are not in the same address space, the command is rejected. The VARY TCPIP,,DROP command drops only established TCP connections, not UDP sockets.

Using the command to drop all connections for a server

If you want to use this function, perform the task in Table 29.

Table 29. Command to drop all connections for a server

Task	Reference
Drop all connections associated with a server by issuing the VARY TCPIP,,DROP command. Indicate the server by specifying the appropriate values on the PORT, JOBNAME, or ASID parameters.	VARY TCPIP,,DROP in *z/OS Communications Server: IP System Administrator's Commands*

Control joining the sysplex XCF group

In z/OS V1R12 Communications Server, you can use a new configuration parameter to prevent a TCP/IP stack from automatically joining the sysplex group at startup. The TCP/IP stack can join the sysplex group at a later time when you issue the VARY TCPIP,,SYSPLEX,JOINGROUP command.

Restriction: The TCP/IP stack must be V1R12 or later to use this function.

Controlling joining the sysplex XCF group

If you want to control whether the TCP/IP stack joins the sysplex XCF group, perform the appropriate tasks in Table 30.

Table 30. Control joining the sysplex XCF group

Task	Reference
Configure the NOJOIN keyword on the SYSPLEXMONITOR parameter of the GLOBALCONFIG statement in the TCP/IP profile.	• GLOBALCONFIG statement in *z/OS Communications Server: IP Configuration Reference*
If you want the stack to join the sysplex group at a later time, issue the VARY TCPIP,,SYSPLEX,JOINGROUP command.	VARY TCPIP,,SYSPLEX in *z/OS Communications Server: IP System Administrator's Commands*

Extension of the retry time limit for CSSMTP

In z/OS V1R12 Communications Server, you can specify a longer total time for Communications Server SMTP (CSSMTP) to use when attempting to re-send mail messages that are not immediately deliverable. In z/OS V1R11 Communications Server, the total time limit was 2 hours. In z/OS V1R12 Communications Server, the total time limit is 120 hours (5 days).

Using the extension of the retry time limit for CSSMTP

If you want to use the longer retry time limit, perform the task in Table 31.

Table 31. Extension of the retry time limit for CSSMTP

Task	Reference
Specify larger values on the RetryLimit statement in the CSSMTP configuration file.	• CSSMTP configuration statements in *z/OS Communications Server: IP Configuration Reference*

SNA and Enterprise Extender

z/OS V1R12 Communications Server includes enhancements to SNA and Enterprise Extender (EE) in the following areas:

- "Enterprise Extender connection health verification"
- "Multipath control for Enterprise Extender" on page 45
- "Improved recovery from RTP pipe stalls" on page 45
- "Enhancements to topology database diagnostics" on page 45

Enterprise Extender connection health verification

z/OS V1R12 Communications Server provides the option to verify the health of an Enterprise Extender (EE) connection by sending an LDLC probe to the remote partner using all five ports. You can verify the connection at activation only or during activation and periodically while the connection is active. During activation, if the LDLC probe cannot reach a port for any reason, you cannot activate the connection and you will receive an error message. If the remote partner does not support an LDLC probe, VTAM issues an error message and activates the connection. If periodic checking is enabled and an LDLC probe is supported but the LDLC probe cannot reach a port for any reason, VTAM issues an error message.

Using Enterprise Extender connection health verification

If you want to use this function, perform the appropriate tasks in Table 32.

Table 32. Enterprise Extender connection health verification

Task	Reference
Set health check verification for all EE connections by specifying the following values on the EEVERIFY start option: • ACTIVATE to verify at activation • *nnn* to verify at activation and periodically • NEVER to turn off verification	EEVERIFY start option in *z/OS Communications Server: SNA Resource Definition Reference*
Set health verification for a specific EE connection. • For EE connection networks, define EEVERIFY on the connection network GROUP definition statements in the EE XCA major node. • For dial-in EE connections that have their associated PUs dynamically created, define EEVERIFY on the model major node (DYNTYPE=EE) PU definition statement. • For predefined EE connections, define EEVERIFY on the PU definition statement in the switched major node.	See the following topics in *z/OS Communications Server: SNA Resource Definition Reference*: • XCA major node operand EEVERIFY • Model major node operand EEVERIFY • Switched major node operand EEVERIFY
Modify the EEVERIFY start option. Issue the MODIFY *procname*, VTAMOPTS,EEVERIFY=*value* command.	MODIFY VTAMOPTS command in *z/OS Communications Server: SNA Operation*
Display the EEVERIFY start option. Issue the DISPLAY NET,VTAMOPTS,OPTION=EEVERIFY or the DISPLAY NET,VTAMOPTS command.	DISPLAY VTAMOPTS command in *z/OS Communications Server: SNA Operation*
Display all active connections that failed EE health verification on their most recent LDLC probe. Issue the DISPLAY NET,EE,LIST=EEVERIFY command.	DISPLAY EE command in *z/OS Communications Server: SNA Operation*
Display the EE health information for the last LDLC probe that was sent to the partner. Issue the DISPLAY NET,EE,ID= command or the DISPLAY NET,EE command; specify either a host name pair or an IP address pair.	DISPLAY EE command in *z/OS Communications Server: SNA Operation*

Multipath control for Enterprise Extender

Before z/OS V1R12 Communications Server, you could code the MULTIPATH statement in the TCP/IP profile to enable multipath support for IP packets across all connections. You might want to enable multipath support for TCP connections but not for Enterprise Extender (EE) connections. In z/OS V1R12 Communications Server, you can use the VTAM start option MULTPATH to control the multipath function for EE.

Controlling the multipath function for EE

To control the multipath function for EE connections, perform the appropriate tasks in Table 33.

Table 33. Multipath control for Enterprise Extender

Task	Reference
The multipath function is disabled by default for EE connections; you do not have to perform any tasks to keep this behavior. Optionally, code the VTAM start option MULTPATH=NO.	MULTPATH start option in *z/OS Communications Server: SNA Resource Definition Reference*
Enable multipath for EE by coding the VTAM start option MULTPATH=TCPVALUE. Multipath has to be enabled in the IP stack as well in order for multipath for EE to be enabled.	MULTPATH start option in *z/OS Communications Server: SNA Resource Definition Reference*

Improved recovery from RTP pipe stalls

z/OS V1R12 Communications Server provides local and path MTU discovery to learn the correct MTU size for Enterprise Extender (EE) connections. The updated information is used to update the link size for the EE connection. If the EE connection is one hop of a high performance routing (HPR) connection, this updated MTU size information is not propagated to the remaining HPR path. This function updates the HPR connection with the updated link size.

Enhancements to topology database diagnostics

The APPN topology database update (TDU) processing was enhanced in z/OS V1R11 Communications Server; see "APPN topology database update enhancements" on page 90. It is further enhanced in z/OS V1R12 Communications Server to include additional diagnostic information and new diagnostic displays.

Using the new topology database diagnostics

If you want to use this function, perform the appropriate tasks in Table 34.

Table 34. Enhancements to topology database diagnostics

Task	Reference
Display a summary of TDU diagnostic information by issuing the DISPLAY NET,TOPO,LIST=TDUDIAG command.	• DISPLAY TOPO command in *z/OS Communications Server: SNA Operation* • DISPLAY TDU information in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*
Display the TDU diagnostic information associated with a node by issuing the DISPLAY NET,TOPO,ID=*node_cpname*,LIST=TDUDIAG command.	DISPLAY TOPO command in *z/OS Communications Server: SNA Operation*
Display the TDU diagnostic information associated with a transmission group (TG) by issuing the DISPLAY NET,TOPO,ORIG=*orig_cpname*,DEST=*dest_cpname*,TGN=*tg_num*,LIST=TDUDIAG command.	DISPLAY TOPO command in *z/OS Communications Server: SNA Operation*

System management and monitoring

z/OS V1R12 Communications Server includes enhancements to system management and monitoring in the following areas:

- "Performance improvement to TCP/IP callable NMI (EZBNMIFR) GetConnectionDetail request"
- "Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics"
- "SMF event records for sysplex events" on page 47
- "Management data for CSSMTP" on page 47
- "Data trace records for socket data flow start and end" on page 49
- "Enhancements to the TN3270E server - session manager sends CV64" on page 49
- "Operator command to query and display OSA information" on page 50
- "Packet trace filtering for encapsulated packets" on page 50
- "Verify Netstat message catalog synchronization" on page 51
- "Enhancements to the TCP/IP storage display" on page 51
- "Enhancements to SNMP manager API" on page 51

Performance improvement to TCP/IP callable NMI (EZBNMIFR) GetConnectionDetail request

z/OS V1R12 Communications Server enhances the GetConnectionDetail request of the TCP/IP callable network management interface (NMI) request to reduce its CPU utilization. This enhancement is provided when all the filters that are specified for the request contain the complete identification (4-tuple) of established TCP connections. The 4-tuple of a TCP connection consists of the local IP address, local port, remote IP address, and remote port for the connection.

There are no tasks to use this function; it is automatically enabled.

Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics

z/OS V1R12 Communications Server provides new TCP/IP callable NMI requests for the following TCP/IP stack information:

- Network interface information
- Network interface and global statistics

Network management applications can use the request output to monitor interface status and TCP/IP stack activity. z/OS V1R12 Communications Server provides the following new requests:

GetGlobalStats
Provides TCP/IP stack global counters for IP, ICMP, TCP, and UDP processing.

GetIfs Provides TCP/IP network interface attributes and IP addresses.

GetIfStats
Provides TCP/IP network interface counters.

GetIfStatsExtended
Provides data link control (DLC) network interface counters.

Using the enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics

If you want to use this function, perform the task in Table 35.

Table 35. Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics

Task	Reference
Develop or enhance an application to obtain TCP/IP network interface information and network interface and global statistics from the TCP/IP callable NMI.	TCP/IP callable NMI (EZBNMIFR) in *z/OS Communications Server: IP Programmer's Guide and Reference*

SMF event records for sysplex events

z/OS V1R12 Communications Server introduces new SMF 119 event records (subtypes 32 – 37), which provide sysplex event notification to describe the following events:

- DVIPA status change (subtype 32)
- DVIPA removed (subtype 33)
- DVIPA target added (subtype 34)
- DVIPA target removed (subtype 35)
- DVIPA target server started (subtype 36)
- DVIPA target server ended (subtype 37)

The new SMF 119 event records are written to the MVS SMF data sets; you can obtain them from the real-time TCP/IP network monitoring Network Management Interface (NMI) (SYSTCPSM).

Using the SMF event records for sysplex events

If you want to use this function, perform the appropriate tasks in Table 36.

Table 36. SMF event records for sysplex events

Task	Reference
Configure SMF logging of the new SMF 119 event records, subtypes 32 – 37, which provide sysplex event information. Specify SMFCONFIG TYPE119 DVIPA in the PROFILE.TCPIP configuration file.	SMFCONFIG statement in *z/OS Communications Server: IP Configuration Reference*
Configure the real-time TCP/IP network monitoring NMI (SYSTCPSM) to support the new SMF 119 event records, subtypes 32 – 37, which provide sysplex event information. Specify NETMONITOR SMFSERVICE DVIPA in the PROFILE.TCPIP configuration file.	NETMONITOR statement in *z/OS Communications Server: IP Configuration Reference*
Enable applications to obtain the new SMF 119 event records, subtypes 32 – 37, from the real-time TCP/IP network monitoring NMI (SYSTCPSM). Configure the user IDs associated with the applications to access the SYSTCPSM NMI interface.	Real-time TCP/IP network monitoring NMI: Configuration and enablement in *z/OS Communications Server: IP Programmer's Guide and Reference*
Verify the SMFCONFIG and NETMONITOR SMFSERVICE settings using the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*

Management data for CSSMTP

z/OS V1R12 Communications Server provides the following new SMF 119 record subtypes, which improve the management of the Communications Server SMTP (CSSMTP) application:

- CSSMTP configuration data records (subtype 48)
- CSSMTP target server connection records (subtype 49)
- CSSMTP mail records (subtype 50)
- CSSMTP spool records (subtype 51)
- CSSMTP statistics records (subtype 52)

Applications that process the new SMF 119 subtypes obtain them using a traditional MVS SMF exit routine or obtain them in real time from the z/OS Communications Server Network Management Interface (NMI) for SMF, SYSTCPSM.

CSSMTP issues the SIOCSAPPLDATA ioctl call to add application data (ApplData) to the TCP connections that are used to connect to target mail servers. You can see the ApplData displayed in the Netstat All/-A, AllConn/-a, and Conn/-c reports. The ApplData is also available from the GetTCPListeners and GetConnectionDetail requests of the TCP/IP callable NMI (EZBNMIFR), and from some SMF 119 records. See *z/OS Communications Server: IP Programmer's Guide and Reference* for the format of the application data for CSSMTP.

Using the management data for CSSMTP

If you want to use the SMF real-time data collection, perform the appropriate tasks in Table 37.

Table 37. NMI enhancements - CSSMTP events using the NMI real-time SMF events

Task	Reference
Configure SMF logging of the new SMF 119 event records, subtypes 48 – 52, which provide CSSMTP event information. Specify the SMF119 statement in the CSSMTP configuration file.	SMF119 statement in *z/OS Communications Server: IP Configuration Reference*
Configure the real-time TCP/IP network monitoring NMI (SYSTCPSM) to support the new SMF 119 event records, subtypes 48 – 52, which provide CSSMTP event information. Specify the NETMONITOR SMFSERVICE CSSMTP statement or the NETMONITOR SMFSERVICE CSMAIL statement in the PROFILE.TCPIP configuration file.	NETMONITOR statement in *z/OS Communications Server: IP Configuration Reference*
Enable applications to obtain the new SMF 119 event records, subtypes 48 – 52, from the real-time TCP/IP network monitoring NMI (SYSTCPSM). Configure the user IDs associated with the applications to access the SYSTCPSM NMI interface.	Real-time TCP/IP network monitoring NMI: Configuration and enablement in *z/OS Communications Server: IP Programmer's Guide and Reference*
Verify the NETMONITOR SMFSERVICE settings using the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*

CSSMTP updates the application data that is associated with each client connection that has a target server. The data consists of the external writer name, the mail server type, and the TLS parameters.

There are no tasks to enable application data; application data collection is always enabled. If you want to display or monitor the application data, perform the tasks in Table 38 on page 49.

Table 38. CSSMTP and application data

Task	Reference
Display the application data using the Netstat COnn/-c command with the APPLDATA modifier.	• See the following topics in *z/OS Communications Server: IP System Administrator's Commands*: – DISPLAY TCPIP,,NETSTAT – The z/OS UNIX netstat command syntax • Application data in *z/OS Communications Server: IP Programmer's Guide and Reference*
Obtain application data by using an NMI application to retrieve the data from the TCP connection termination SMF record or use the NMI callable routine GetConnectionDetail request.	Network management interfaces in *z/OS Communications Server: IP Programmer's Guide and Reference*

Data trace records for socket data flow start and end

z/OS V1R12 Communications Server enhances TCP/IP data tracing (DATTRACE) to provide two new trace records for processing associated with TCP and UDP sockets:

- A start record with the State field `API Data Flow Starts`, which indicates that the first data was sent or received by the application for the associated TCP or UDP socket.
- An end record with the State field `API Data Flow Ends`, which indicates that the socket has been closed.

Restriction: The socket data flow start and end data trace records are not supported for RAW sockets.

Using the data trace records for socket data flow start and end

If you want to use this function, perform the appropriate tasks in Table 39.

Table 39. Data trace records for socket data flow start and end

Task	Reference
Obtain the new start and end data trace records from the real-time TCP/IP packet trace and the data trace NMI.	Format of service-specific data in *z/OS Communications Server: IP Programmer's Guide and Reference*
Format the new start and end data trace records.	Formatting data traces using IPCS in *z/OS Communications Server: IP Diagnosis Guide*

Enhancements to the TN3270E server - session manager sends CV64

In z/OS V1R12 Communications Server, VTAM provides applications the ability to pass IP information. An application, such as a session manager, can use this function to inform VTAM and its session partner of any IP characteristics (such as IP address or port number) that are associated with the resource that the application is representing. This function enables VTAM displays of the IP information, and it can enable additional PLU functionality.

Using the new session manager CV64 function

If you want to use this function, perform the appropriate tasks in Table 40 on page 50.

Table 40. Enhancements to the TN3270E server - session manager sends CV64

Task	Reference
Modify your application to pass IP information through a TCP/IP Information Control Vector (CV64) to VTAM by updating the OPEN ACB and SETLOGON START invocations of the application.	Supplying control vectors with the SETLOGON START in *z/OS Communications Server: SNA Programming*
Verify that the application is passing in IP information by issuing the DISPLAY NET,ID= command. Specify the resource name and ensure that the IST1669I message is present in the output, when appropriate.	See DISPLAY ID command in *z/OS Communications Server: SNA Operation* for a sample of a display containing IP information.

Operator command to query and display OSA information

z/OS V1R12 Communications Server provides a new DISPLAY TCPIP,,OSAINFO command that you can use to retrieve information about an interface from an OSA-Express feature that is in QDIO mode. The new command is an alternative to using OSA/SF, which lacks information about many of the latest enhancements to the OSA-Express feature and to z/OS Communications Server.

Restrictions: Unlike OSA/SF, a single DISPLAY TCPIP,,OSAINFO command can display only information for a single OSA-Express interface. The interface must be defined and active in the stack in which the command is issued.

Dependencies: This function is limited to OSA-Express3 Ethernet features that are in QDIO mode and that are running on a minimum of an IBM System z10. See the 2097DEVICE and the 2098DEVICE Preventive Service Planning (PSP) buckets for further information.

Using the operator command to query and display OSA information

If you want to use this function, perform the task in Table 41.

Table 41. Operator command to query and display OSA information

Task	Reference
Issue the DISPLAY TCPIP,,OSAINFO command to determine general information about an OSA-Express feature, including information registered to the OSA-Express feature by the TCP/IP stack.	DISPLAY TCPIP,,OSAINFO in *z/OS Communications Server: IP System Administrator's Commands*

Packet trace filtering for encapsulated packets

In z/OS V1R12 Communications Server, the following packet trace improvements are included:

- Packet trace filtering is available to encapsulated packets that are used in VIPAROUTE traffic.
- The next-hop IP address is included on the trace output. This address can be obtained from the fully formatted packet trace using the Interactive Problem Control System (IPCS). The next-hop IP address is also available to applications that use the real-time packet trace through the real-time TCP/IP networking monitoring API.

Packet trace filtering is available for encapsulated packets. For example, sysplex distributor using VIPAROUTE must encapsulate the original packet with a new header that defines the source and destination addresses as the sysplex distributor and target. Before z/OS V1R12 Communications Server, packet trace filtering looked at only the outer header, which made it impossible to filter by the original

source (of the client) or destination IP address (of the DVIPA). In z/OS V1R12 Communications Server, if a packet is encapsulated, packet trace filtering examines the inner header to filter the encapsulated packet by the original source or destination IP address.

Dependencies: The next-hop information is shown only in the fully formatted packet trace. If IPCS is used to format the packet trace, the report type must be set to FULL.

If you want to use this function, perform the appropriate tasks in Table 42.

Table 42. Packet trace filtering for encapsulated packets

Task	Reference
To view the next-hop IP address in the packet trace header using IPCS, specify the report type FULL in the IPCS CTRACE option.	Formatting component traces in *z/OS Communications Server: IP Diagnosis Guide*

Verify Netstat message catalog synchronization

In z/OS V1R12 Communications Server, the Netstat command provides support to verify that the message catalogs that are being used are at the correct level when the message catalog is opened. This function prevents Netstat from abending or not functioning correctly when the message catalog is out of synch with the Netstat command.

Verifying Netstat message catalog synchronization

If you want to use this function, perform the task in Table 43.

Table 43. Verify Netstat message catalog synchronization

Task	Reference
To customize the Netstat message catalogs, follow the steps described in the referenced topics.	Customizing TCP/IP messages in *z/OS Communications Server: IP Configuration Guide*

Enhancements to the TCP/IP storage display

In z/OS V1R12 Communications Server, the DISPLAY TCPIP,,STOR command display and the NMI storage statistics report are enhanced to distinguish the common storage that is used by dynamic LPA for load modules from the ECSA storage that is used for control blocks.

Using the enhancements to the TCP/IP storage display

If you want to use this function, perform the task in Table 44.

Table 44. Enhancements to the TCP/IP storage display

Task	Reference
Display TCP/IP storage statistics.	DISPLAY TCPIP,,STOR in *z/OS Communications Server: IP System Administrator's Commands*

Enhancements to SNMP manager API

z/OS V1R12 Communications Server extends the SNMP manager API so that the API can do the following tasks:

- Create and retrieve SNMP values of type UNSIGNED32.
- Configure an authoritative engine ID for SNMPv3 traps. Currently, the SNMP manager API creates its own SNMPv3 authoritative engine ID, part of which is a randomized value. A configured authoritative engine ID can be used with SNMP trap receiver applications so that the trap receiver applications recognize specific SNMP manager API applications when they are processing SNMPv3 traps.

Using the enhancements to SNMP manager API

If you want to use this function, perform the appropriate tasks in Table 45.

Table 45. Enhancements to SNMP manager API

Task	Reference
Create an SNMP value of type UNSIGNED32 by calling the snmpValueCreateUnsigned32() function from your manager application.	SNMP manager API functions in *z/OS Communications Server: IP Programmer's Guide and Reference*
Implement the engine ID function by specifying an authoritative engine ID parameter for each SNMPv3 entry in your SNMP Manager API configuration file.	SNMP manager API configuration file in *z/OS Communications Server: IP Programmer's Guide and Reference*

Chapter 4. V1R11 new function summary

This information contains topics about every function or enhancement introduced in z/OS V1R11 Communications Server. Each function is described and the following information is presented if applicable:

- Restrictions, dependencies, and coexistence considerations of the function
- A task table that identifies the actions necessary to use the function
- References to the documents that contain more detailed information

See Table 8 on page 21 for a complete list of the functional enhancements.

See *z/OS Migration* for information about how to migrate and maintain the functional behavior of previous releases.

See *z/OS Summary of Message and Interface Changes* for information about new and changed messages and interfaces.

Support considerations in V1R11

z/OS V1R11 Communications Server removes support for the following functions:

- Boot Information Negotiation Layer (BINL) server function
- Berkeley Internet Name Domain 4.9.3 (BIND 4.9.3) DNS server, including the Connection Optimization (DNS/WLM) function
- Dynamic Host Configuration Protocol (DHCP) server function
- Network Database (NDB) server function

See *z/OS Migration* for detailed information about all the z/OS V1R11 Communications Server support considerations.

General release considerations in V1R11

In addition to the function-specific updates, z/OS V1R11 Communications Server introduces the following changes:

- Each router using OSPF has a 32-bit router ID that uniquely identifies it within an OSPF autonomous system. If multiple routers use the same router ID, routing problems including adjacency failures and packet loss can occur. OMPROUTE issues message EZZ8165I when it detects another OSPF router that is using the same router ID as OMPROUTE.
- The trace resolver output includes additional time stamps when communicating with a Domain Name System (DNS) server. You can use this information to identify domain name servers that are responding slowly or not at all to resolver queries.
- Netstat connection reports include TCP connections in SynRcvd state.

Application integration, data consolidation, and standards

The following topics enhance application integration, data consolidation, and standards:

- "New SMTP client for sending Internet mail" on page 54
- "FTP enhancements" on page 56

- "Customizable pre-logon banner for otelnetd" on page 63
- "Remote execution server enhancements" on page 63
- "TN3270 support of TSO logon reconnect" on page 64
- "IPv6 stateless address autoconfiguration enhancements" on page 64
- "New API to obtain IPv4 network interface MTU" on page 66
- "RFC 5095 deprecation of IPv6 type 0 route header" on page 66
- "CICS sockets enhancements" on page 67

New SMTP client for sending Internet mail

z/OS V1R11 Communications Server introduces a new mail-forwarding SMTP client application called Communications Server SMTP (CSSMTP). CSSMTP processes spool files on the JES spool data set that contain mail messages and forwards the mail messages to target message transfer agents (MTAs) without resolving each recipient.

If you currently use MVS batch jobs to send bulk mail by way of SMTPD, you can use CSSMTP to offload this mail. CSSMTP can improve the performance, scalability, and availability for the client function of SMTPD, but it does not act as a listening MTA server like SMTPD; CSSMTP can send mail to the Internet from z/OS, but it cannot receive mail from the Internet into z/OS.

CSSMTP can coexist with SMTPD and multiple instances of CSSMTP can run on a single host.

CSSMTP implements RFC 2821 and RFC 2822 for interacting with server MTAs, and it supports additional RFCs for message size (RFC 1870) and security (RFC 3207).

If you are currently using Communications Server SMTPD on z/OS, you should consider using CSSMTP. See the information about differences between CSSMTP and SMTPD in *z/OS Communications Server: IP Configuration Guide* for more information about moving from the SMTPD to the CSSMTP application.

Dependencies: If you are using Transport Layer Security (TLS) to provide private, authenticated communication over the Internet, you need to configure TLS on the CSSMTP application and the target server. See RFC 3207 *SMTP Service Extension for Security SMTP over TLS* for details. Ensure that the CSSMTP application and the target server are configured the same way for secure mail. See the information about enabling the SMTP server and client to use Transport Layer Security (TLS) in *z/OS Communications Server: IP Configuration Guide* for details.

Using the new SMTP client for sending Internet mail

If you want to use this function, perform the appropriate tasks in Table 46 on page 55.

Table 46. New SMTP client for sending Internet mail

Task	Procedure	Reference
Configure the CSSMTP application.	Create the file manually using a text editor or copy and modify the sample provided in CSSMTPCF in SEZAINST.	• Communications Server SMTP application statement in *z/OS Communications Server: IP Configuration Reference* • Configuring the CSSMTP application in *z/OS Communications Server: IP Configuration Guide* • The CSSMTPCF configuration sample included in SEZAINST
Configure JES2 or JES3.	Perform the following steps: 1. Ensure that CSSMTP interfaces with JES APIs to create, read, write, and purge data from the JES spool data set. 2. Set JES initialization parameters correctly so that mail can be sent to CSSMTP.	Steps for JES setup in *z/OS Communications Server: IP Configuration Guide*
Optionally, set up security authorization to control who can start, stop, or issue the modify commands for the CSSMTP application.	See *z/OS Communications Server: IP Configuration Guide* for information on setting up this security authorization.	• If the security product being used is RACF, see *z/OS Security Server RACF Security Administrator's Guide* information regarding RACF controls for the start, stop, and modify commands. • Steps for granting authority to start CSSMTP in *z/OS Communications Server: IP Configuration Guide*
Optionally, control access to CSSMTP by defining the necessary SERVAUTH profiles and permitting authorized users to these profiles for an external writer name.	See *z/OS Communications Server: IP Configuration Guide* and the EZARACF sample in SEZAINST for information on setting RACF for CSSMTP.	• See the information about controlling which users can send mail by way of CSSMTP by restricting the user IDs in Security for CSSMTP (optional) in *z/OS Communications Server: IP Configuration Guide* • ExtWrtName statement in *z/OS Communications Server: IP Configuration Reference*
If you want to check and subsequently accept or reject mail outbound from the JES spool file, write and activate the CSSMTP user exit program.	Use the sample VERSION3 user exit CSSMTPV3 in SEZAINST.	CSSMTP exit in *z/OS Communications Server: IP Configuration Reference*

Table 46. New SMTP client for sending Internet mail (continued)

Task	Procedure	Reference
Create mail on the spool file.	Examples: • Use the SMTPNOTE CLIST to prepare mail using the Time Sharing Option (TSO) EDIT command or to send mail that is created with another system editor. • Issue an XMIT command, which sends a previously constructed mail file containing SMTP commands for one or more mail messages. The mail file is sent to the spool file to be processed by CSSMTP. • Use the IEBGENER utility to copy a mail file to a JES sysout file.	Sending electronic mail using the Communications Server SMTP application in *z/OS Communications Server: IP User's Guide and Commands*
Customize the SMTPNOTE CLIST.	Copy and customize the SMTPNOTE CLIST on every system on which users will be able to send mail with the SMTPNOTE CLIST. **Tips:** • SMTPNOTE uses the TSO transmit (XMIT) command to interface with CSSMTP. • There is a sample for SMTPNOTE in SEZAINST member SMTPNOTE.	Steps for customizing the SMTPNOTE CLIST (optional) in *z/OS Communications Server: IP Configuration Guide*
Depending on your network design, determine whether AT-TLS will be used to secure some or all of the connections for mail between CSSMTP clients and servers.	Determine which CSSMTP target servers (if used) will have TLS to provide private, authenticated communication over the Internet. See RFC 3207 *SMTP Service Extension for Security SMTP over TLS* for details.	See the following topics in *z/OS Communications Server: IP Configuration Guide* • Application Transparent Transport Layer Security data protection • Steps for using Transport Layer Security for CSSMTP
Start CSSMTP if not already started.	Create a new data set member in your procedure library for the CSSMTP JCL.	• Steps for configuring and starting CSSMTP in *z/OS Communications Server: IP Configuration Guide* • The CSSMTPCF configuration sample included in SEZAINST

FTP enhancements

The FTP enhancements include the following topics:

- "FTP access to UNIX named pipes"
- "FTP large-volume access" on page 61
- "FTP passive mode enhancements" on page 61

FTP access to UNIX named pipes

In z/OS V1R11 Communications Server, FTP can transfer files to and from z/OS UNIX System Services named pipes.

Applications that support reading from named pipes can process data that is transferred into a named pipe while FTP is still writing data into the named pipe. Likewise, FTP can initiate the transfer of data that is written to or from a named

pipe while an application is still writing to or from the named pipe. Applications that support reading from and writing to named pipes benefit because of the following reasons:

- An I/O transfer to a named pipe is faster than an I/O transfer to a regular z/OS UNIX System Services file.
- Applications can run simultaneously with file transfers.

Restrictions:

- Anonymous users cannot create, rename, delete, read from, or write to named pipes in the FTP server z/OS UNIX System Services file system.
- You can append to but not replace the contents of a named pipe.
- The operating system provides no serialization for z/OS UNIX named pipes. Multiple processes can read from or write to a named pipe.

Using the FTP access to UNIX named pipes: If you want to use this function, perform the appropriate tasks in Table 47.

Table 47. FTP access to UNIX named pipes

Task	Procedure	Reference
Determine whether a named pipe exists in the FTP server UNIX file system.	From the z/OS FTP client, issue one of the following subcommands to list the contents of the directory where you expect the named pipe: • DIr • LS	See the following topics in *z/OS Communications Server: IP User's Guide and Commands*: • DIr subcommand–Obtain a list of directory entries • LS subcommand–Obtain a list of file names Also see Displaying file and directory permissions in *z/OS UNIX System Services User's Guide*
Use an FTP client to create a named pipe on a z/OS FTP server host for later use.	Do one of the following: • From the z/OS FTP client, issue the MKFifo subcommand. • From any FTP client, issue the QUOte subcommand to send an XFIF<*pathname*> command to the server. This named pipe will not contain any data.	See the following topics in *z/OS Communications Server: IP User's Guide and Commands*: • MKFifo subcommand • Using z/OS UNIX System Services named pipes
Control the file permissions that are assigned to named pipes created by z/OS FTP in the server file system.	Do one of the following to configure the server UMASK value: • Code the UMASK statement in the FTP.DATA file before starting the server. • From the z/OS FTP client, issue the SIte subcommand to set the server UMASK value for the current session. • From any FTP client, issue the QUOte subcommand to send a SITE command with the UMASK parameter to the server.	UMASK (FTP client and server) statement in *z/OS Communications Server: IP Configuration Reference* Also see the following topics in *z/OS Communications Server: IP User's Guide and Commands*: • SIte subcommand—Send site-specific information to a host • QUOte subcommand—Send an uninterpreted string of data

Table 47. FTP access to UNIX named pipes (continued)

Task	Procedure	Reference
Change the file permissions that are assigned to a named pipe while you are logged into the z/OS FTP server on the target host.	Do one of the following: • From the z/OS FTP client, issue the SIte subcommand with the CHMOD parameter. • From any FTP client, issue the QUOte subcommand to send a SITE command with the CHMOD parameter to the server.	See the following topics in *z/OS Communications Server: IP User's Guide and Commands*: • SIte subcommand—Send site-specific information to a host • QUOte subcommand—Send an uninterpreted string of data
Transfer data into a named pipe on a z/OS FTP server host.	Perform the following steps: 1. Configure the server for named pipe transfer. 2. If you are using the z/OS FTP client, use the SUnique subcommand to toggle the SUnique value to off. 3. Start a process at the FTP server host to read from the named pipe. 4. Store or append a file to the named pipe on the server host.	See the following topics in *z/OS Communications Server: IP User's Guide and Commands*: • SUnique subcommand–Changes the storage method • Using z/OS UNIX System Services named pipes Also see the following topics in *z/OS Communications Server: IP Configuration Reference*: • UNIXFILETYPE (FTP client and server) statement • FIFOOPENTIME (FTP client and server) statement • FIFOIOTIME (FTP client and server) statement
Retrieve data from a named pipe on a z/OS FTP server host.	Perform the following steps: 1. Configure the server for named pipe transfer. 2. Start a process on the FTP server host to write to the named pipe. 3. From the FTP client, issue the Get subcommand to start the file transfer.	Using z/OS UNIX System Services named pipes in *z/OS Communications Server: IP User's Guide and Commands*. Also see the following topics in *z/OS Communications Server: IP Configuration Reference*: • UNIXFILETYPE (FTP client and server) statement • FIFOOPENTIME (FTP client and server) statement • FIFOIOTIME (FTP client and server) statement

Table 47. FTP access to UNIX named pipes (continued)

Task	Procedure	Reference
Configure the server for named pipe transfer.	Configure these values at the FTP server: • UNIXFILETYPE FIFO • FIFOOPENTIME • FIFOIOTIME Do one of the following to configure these values: • Code the following statements in FTP.DATA before starting the server: – UNIXFILETYPE FIFO – FIFOIOTIME – FIFOOPENTIME • From the z/OS FTP client, issue the SIte subcommand with the UNIXFILETYPE, FIFOIOTIME, and FIFOOPENTIME parameters. • From any FTP client, issue the QUOte subcommand to send SITE commands to the server with the UNIXFILETYPE, FIFOIOTIME, and FIFOOPENTIME parameters.	See the following topics in *z/OS Communications Server: IP Configuration Reference*: • UNIXFILETYPE (FTP client and server) statement • FIFOOPENTIME (FTP client and server) statement • FIFOIOTIME (FTP client and server) statement See the following topics in *z/OS Communications Server: IP User's Guide and Commands*: • SIte subcommand—Send site-specific information to a host • QUOte subcommand—Send an uninterpreted string of data • Using z/OS UNIX System Services named pipes
Display the server settings for the following configuration options: • UNIXFILETYPE • FIFOOPENTIME • FIFOIOTIME	Do one of the following: • From the z/OS FTP client, issue one of the following subcommands: – STAt – STAt (UNIXFILETYPE – STAt (FIFOOPENTIME – STAt (FIFOIOTIME • From any FTP client, issue the QUOte subcommand to send one of the following commands to the FTP server: – STAT – XSTA (UNIXFILETYPE	STAtus subcommand—Retrieve status information from a remote host in *z/OS Communications Server: IP User's Guide and Commands*
Control the file permissions that are assigned to named pipes that are created by z/OS FTP on the client host.	Do one of the following to configure the server UMASK value: • Code the UMASK statement in the client FTP.DATA before starting the client. • From the z/OS FTP client, issue the LOCSIte subcommand to set the client UMASK value for the current session.	• UMASK (FTP client and server) statement in *z/OS Communications Server: IP Configuration Reference* • LOCSIte subcommand—Specify site information to the local host in *z/OS Communications Server: IP User's Guide and Commands*
Change the file permissions that are assigned to a named pipe on the FTP client host.	Issue the LOCSIte subcommand with the CHMOD parameter.	LOCSIte subcommand—Specify site information to the local host in *z/OS Communications Server: IP User's Guide and Commands*

Table 47. FTP access to UNIX named pipes (continued)

Task	Procedure	Reference
Transfer data into a named pipe on a z/OS FTP client host.	Perform the following steps: 1. Configure the client for named pipe transfer. 2. Start a process at the FTP client host to read from the named pipe. 3. From the FTP client, issue the Get or MGet subcommand	Using z/OS UNIX System Services named pipes in *z/OS Communications Server: IP User's Guide and Commands*. Also see the following topics in *z/OS Communications Server: IP Configuration Reference*: • UNIXFILETYPE (FTP client and server) statement • FIFOOPENTIME (FTP client and server) statement • FIFOIOTIME (FTP client and server) statement
Send data from a named pipe on a z/OS FTP client host.	Perform the following steps: 1. Configure the client for named pipe transfer. 2. Start a process on the FTP client host to write to the named pipe. 3. From the FTP client, issue the Put, MPut, or APPEnd subcommand to start the file transfer.	Using z/OS UNIX System Services named pipes in *z/OS Communications Server: IP User's Guide and Commands*. Also see the following topics in *z/OS Communications Server: IP Configuration Reference*: • UNIXFILETYPE (FTP client and server) statement • FIFOOPENTIME (FTP client and server) statement • FIFOIOTIME (FTP client and server) statement
Configure the client for named pipe transfer.	Configure the following values at the FTP client: • UNIXFILETYPE FIFO • FIFOOPENTIME • FIFOIOTIME Do one of the following to configure these values: • Code the following statements in FTP.DATA before starting the client: – UNIXFILETYPE FIFO – FIFOIOTIME – FIFOOPENTIME • From the z/OS FTP client, issue the LOCSIte subcommand with the UNIXFILETYPE, FIFOIOTIME, and FIFOOPENTIME parameters.	See the following topics in *z/OS Communications Server: IP Configuration Reference*: • UNIXFILETYPE (FTP client and server) statement • FIFOOPENTIME (FTP client and server) statement • FIFOIOTIME (FTP client and server) statement Also see the following topics in *z/OS Communications Server: IP User's Guide and Commands*: • LOCSIte subcommand—Specify site information to the local host • Using z/OS UNIX System Services named pipes
Display the client settings for the following configuration options: • UNIXFILETYPE • FIFOOPENTIME • FIFOIOTIME	From the z/OS FTP client, issue one of the following subcommands: • LOCSTat • LOCSTat UNIXFILETYPE • LOCSTat FIFOOPENTIME • LOCSTat FIFOIOTIME	LOCSTat subcommand—Display local status information in *z/OS Communications Server: IP User's Guide and Commands*

FTP large-volume access

In z/OS V1R11 Communications Server, FTP reports can display space statistics for volumes. The reports are generated by using the QDISK parameter on the following subcommands and command:

- The FTP client LOCSIte and SIte subcommands with the QDISK parameter now use an enhanced format to report space statistics for volumes.
- The FTP server SITE command with the QDISK parameter now uses an enhanced format to report space statistics for volumes.

Using the FTP large-volume access: If you want to use this function, perform the appropriate tasks in Table 48.

Table 48. FTP large-volume access

Task	Procedure	Reference
Display space statistics for one or more volumes on the z/OS FTP client host.	From the z/OS FTP client, issue the LOCSIte subcommand with the QDISK parameter.	LOCSIte subcommand—Specify site information to the local host in *z/OS Communications Server: IP User's Guide and Commands*
Interpret the output by issuing the LOCSIte subcommand with the QDISK parameter.	See *z/OS Communications Server: IP Messages Volume 1 (EZA)* for an explanation of the following messages: • EZA2192I • EZA2193I • EZA2194I	EZA2192I , EZA2193I , and EZA2194I in *z/OS Communications Server: IP Messages Volume 1 (EZA)*
Display space statistics for one or more volumes on the z/OS FTP server host.	After logging into the z/OS FTP server, do one of the following: • From the z/OS FTP client, issue the SIte subcommand with the QDISK parameter. • From any FTP client, issue the QUOte subcommand in one of the following ways: – QUOte SITE QDISK – QUOte SITE QDISK=*volume serial* where *volume serial* is the volume serial number of a volume on the FTP server host.	SIte subcommand—Send site-specific information to a host and QUOte subcommand—Send an uninterpreted string of data in *z/OS Communications Server: IP User's Guide and Commands*

Interpret the server reply to the SITE command when the QDISK parameter is specified.	See *z/OS Communications Server: IP and SNA Codes* for an explanation of the following codes:
	`200-  Percent Free Free  Largest  Free`
	`200- Volume Free  Cyls Trks  Cyls-Trks Exts  Use Attr`
		200- Percent Free Free Largest and 200- Volume Free Cyls Trks Cyls-Trks Exts Use Attr FTP replies in *z/OS Communications Server: IP and SNA Codes*

FTP passive mode enhancements

In z/OS V1R11 Communications Server, the FTP client supports a new configuration option, PASSIVEIGNOREADDR. This option causes the z/OS FTP client to ignore the IP address in the PASV reply when it is establishing a data connection to the FTP server. Instead, the z/OS FTP client uses the IP address it used to log into the FTP server and the port number from the PASV reply to establish the data connection.

The option enables passive mode data connections to succeed when the server is behind Network Address Translation (NAT) processing and might not advertise its correct external IP address to the client.

Restrictions:

- These enhancements generally allow passive mode FTP data connections to be established through NAT firewalls in cases in which EPSV (extended passive mode support) would have done so. If the FTP control connection is secured with SSL/TLS and if the NAT firewalls (in addition to performing NAT) also implement dynamic filters based on the content of the PASV (or EPSV) reply, these enhancements might not be sufficient to allow the connections to be established through the NAT firewalls. In these cases, use the FTP CCC command (clear command channel).
- FTP ignores the PASSIVEIGNOREADDR option during proxy file transfer.

Dependency: The FWFRIENDLY parameter must be set to TRUE for the PASSIVEIGNOREADDR option to have an effect.

Using the FTP passive mode enhancements: If you want to use this function, perform the tasks in Table 49.

Table 49. FTP passive mode enhancements

Task	Procedure	Reference
Enable the FTP client to ignore the IP address in the PASV reply from the server.	Do one of the following: • Code the PASSIVEIGNOREADDR TRUE statement in the FTP client FTP.DATA file. • Issue the LOCSIte subcommand with the PASSIVEIGNOREADDR parameter.	• PASSIVEIGNOREADDR (FTP client) statement in *z/OS Communications Server: IP Configuration Reference* • LOCSIte subcommand—Specify site information to the local host in *z/OS Communications Server: IP User's Guide and Commands*
Configure the client to use the PASV command to establish data connections for file transfer.	Do one of the following: • Code the FWFRIENDLY TRUE statement in the FTP client FTP.DATA file. • Issue the LOCSIte subcommand with the FWFRIENDLY parameter.	• FWFRIENDLY (FTP client) statement in *z/OS Communications Server: IP Configuration Reference* • LOCSIte subcommand—Specify site information to the local host in *z/OS Communications Server: IP User's Guide and Commands*
Determine whether the FTP client uses or ignores the IP address in the PASV reply.	Issue the LOCSTat subcommand. You can use the PASSIVEIGNOREADDR option to limit the display to the PASSIVEIGNOREADDR configuration only.	LOCSTat subcommand—Display local status information in *z/OS Communications Server: IP User's Guide and Commands*
Determine whether the FTP client issues the EPSV command.	Issue the LOCSTat subcommand. You can use the EPSV4 option to limit the display to information about the EPSV4 command only.	LOCSTat subcommand—Display local status information in *z/OS Communications Server: IP User's Guide and Commands*

Table 49. FTP passive mode enhancements (continued)

Task	Procedure	Reference
Enable file transfer through a NAT firewall when the control connection is encrypted and the FTP server does not support the EPSV command.	Perform the following steps: 1. Use the procedure for enabling the FTP client to ignore the IP address in the server's PASV reply. 2. Use the procedure for configuring the client to use the PASV command to establish data connections for file transfer.	See the following topics in *z/OS Communications Server: IP Configuration Reference*: • PASSIVEIGNOREADDR (FTP client) statement • FWFRIENDLY (FTP client) statement Also see LOCSIte subcommand—Specify site information to the local host in *z/OS Communications Server: IP User's Guide and Commands*.

Customizable pre-logon banner for otelnetd

In z/OS V1R11 Communications Server, the z/OS UNIX Telnet server (otelnetd) provides a new banner page that can be displayed prior to the login prompt when a user connects to the server. This new banner page is in addition to the banner page that can be displayed after a user successfully logs into the server.

Restrictions:

- The banner page must be stored in the /etc/otelnetd.banner directory.
- The existing -h parameter disables the display of the new banner page as well as the post-login banner page.

Using the customizable pre-logon banner for otelnetd

If you want to use this function, perform the task in Table 50.

Table 50. Customizable pre-logon banner for otelnetd

Task	Procedure	Reference
Enable the z/OS UNIX Telnet server (otelnetd) to display a banner page before the login prompt is displayed	Perform the following steps: 1. Create the /etc/otelnetd.banner directory. 2. Edit the /etc/otelnetd.banner file to contain your banner page message.	Installation information in *z/OS Communications Server: IP Configuration Guide*

Remote execution server enhancements

When the purge parameter of the MVS remote execution server is set to N (PURGE=N), the server leaves jobs on the JES spool; however, there are other conditions that can cause a job to remain on the spool. z/OS V1R11 Communications Server improves the availability of the MVS remote execution server by polling JES for the status of jobs that are flagged as residing on the spool when the internal job name table is almost full. Job names that represent jobs that have been purged become available for reuse. The polling function is not related to the setting of the PURGE parameter.

The server issues new messages to the console when the server detects that the job name table is getting full. Automation can detect this condition and restart the server if necessary.

Restriction: The remote execution server must be running on an IBM stack.

Using the remote execution server enhancements

If you want to use this function, perform the tasks in Table 51.

Table 51. Remote execution server enhancements

Task	Procedure	Reference
Detect remote execution server resource shortage problems.	Update your operating procedures or your automation product to monitor the new messages EZA4434I and EZA4434E. • Message EZA4434I is issued when approximately 85% of the resources are exhausted. • Message EZA4435E is issued when all the resources are exhausted.	*z/OS Communications Server: IP Messages Volume 1 (EZA)*
Handle remote execution server resource shortage problems.	Perform the appropriate steps: • If message EZA4434I is displayed on the console and if the remote execution server is running with the PURGE=N option specified, do the following: 1. Verify that the server was started with the PURGE=N parameter. 2. Issue the MODIFY command to change the parameter to PURGE=Y. • If message EZA4434I is displayed on the console, check the JES spool and keep purging any accumulated RSH jobs that can be removed from the spool. RSH and REXEC requests will continue to be processed. You should recycle the server as soon as possible. • If message EZA4435E is displayed on the console, check the JES spool and keep purging any accumulated RSH jobs that can be removed from the spool. Stop the RSH server and then start it. **Result:** RSH and REXEC requests will be able to be processed.	• *z/OS Communications Server: IP Configuration Reference* • *z/OS Communications Server: IP Messages Volume 1 (EZA)*

TN3270 support of TSO logon reconnect

z/OS V1R11 Communications Server, in conjunction with TSO/E, provides support for logon reconnect when the LOGONHERE parameter is correctly defined in SYS1.PARMLIB member IKJTSOxx. The logon reconnect will takeover the original TSO session even when the original TSO session is not disconnected. See the following for coding details:

- *z/OS MVS Initialization and Tuning Reference*
- *z/OS TSO/E Customization*

There are no tasks to enable this function; it is automatically enabled.

IPv6 stateless address autoconfiguration enhancements

In z/OS V1R11 Communications Server, a client application can use IPv6 temporary addresses that were automatically configured and that were generated from a random interface ID to address security and privacy concerns identified by RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. The use of temporary addresses with random and changing interface IDs embedded in the address makes it more difficult for eavesdropping software to correlate

independent transactions that use different IPv6 addresses that were automatically configured but that involve the same z/OS system.

Restriction: The use of IPv6 temporary addresses that are automatically configured is restricted to IPAQENET6 interfaces.

Incompatibility: IPv6 temporary addresses that are automatically configured are not generated for an interface that has manually configured IP addresses or prefixes.

Using the IPv6 stateless address autoconfiguration enhancements

If you want to use this function, perform the appropriate tasks in Table 52.

Table 52. IPv6 stateless address autoconfiguration enhancements

Task	Procedure	Reference
Enable the generation of IPv6 temporary addresses for a TCP/IP stack.	Specify the TEMPADDRS parameter on the IPCONFIG6 statement.	• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in *z/OS Communications Server: IPv6 Network and Application Design Guide* • IPCONFIG6 in *z/OS Communications Server: IP Configuration Reference*
Specify the IPv6 prefixes for which IPv6 temporary addresses can be generated for a specific interface (if you need to limit the prefixes for which temporary addresses are generated).	Specify the TEMPPREFIX parameter on the INTERFACE statement.	• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in *z/OS Communications Server: IPv6 Network and Application Design Guide* • INTERFACE — IPAQENET6 OSA-Express QDIO interfaces in *z/OS Communications Server: IP Configuration Reference*
Enable a client application to use IPv6 temporary addresses.	Specify a JOBNAME *jobname* TEMPADDRS entry in the SRCIP statement block.	• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in *z/OS Communications Server: IPv6 Network and Application Design Guide* • SRCIP in *z/OS Communications Server: IP Configuration Reference*
Display stack-level IPv6 temporary address information.	Issue the Netstat CONFIG/-f command to display the stack-level IPv6 temporary address information.	• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in *z/OS Communications Server: IPv6 Network and Application Design Guide* • Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*
Display the IPv6 prefixes for which IPv6 temporary addresses can be generated for an interface.	Issue the Netstat DEVLINKS/-d command to display the IPv6 prefixes for which temporary addresses can be generated for an interface.	• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in *z/OS Communications Server: IPv6 Network and Application Design Guide* • Netstat DEvlinks/-d report in *z/OS Communications Server: IP System Administrator's Commands*

Table 52. IPv6 stateless address autoconfiguration enhancements (continued)

Task	Procedure	Reference
Display the configured SRCIP entries.	Issue the Netstat SRCIP/-J command to display the SRCIP entries.	• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in *z/OS Communications Server: IPv6 Network and Application Design Guide* • Netstat SRCIP/-J report in *z/OS Communications Server: IP System Administrator's Commands*
Display IPv6 temporary addresses that are generated.	Issue the Netstat HOME/-h command to display any temporary addresses that are generated.	• See the discussion on how to configure a TCP/IP stack to generate IPv6 temporary addresses in *z/OS Communications Server: IPv6 Network and Application Design Guide* • Netstat HOme/-h report in *z/OS Communications Server: IP System Administrator's Commands*

New API to obtain IPv4 network interface MTU

In z/OS V1R11 Communications Server, applications can determine the MTU (maximum transmission unit) for a TCP/IP stack IPv4 interface using a new programming interface ioctl. This support is similar to existing support for IPv6 interfaces.

Restriction: This function does not support applications that are using the Pascal application programming interface or the C application programming interface that is provided by TCP/IP.

Using the new API to obtain IPv4 network interface MTU

If you want to use this function, perform the task in Table 53.

Table 53. New API to obtain IPv4 network interface MTU

Task	Procedure	Reference
Determine the MTU for a TCP/IP stack IPv4 interface.	Issue the SIOCGIFMTU ioctl.	• *z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference* • *z/OS Communications Server: IP CICS Sockets Guide* • *z/OS Communications Server: IP IMS Sockets Guide*

RFC 5095 deprecation of IPv6 type 0 route header

In z/OS V1R11 Communications Server, TCP/IP is modified to deprecate support for IPv6 type 0 routing headers. The reason for this deprecation is described in RFC 5095.

There are no tasks to enable this change; it is automatically enabled.

Incompatibility: Any application that uses the IPV6_RTHDR option to build type 0 routing headers in the IPv6 packets that it sends now receives an error when it attempts to do this.

CICS sockets enhancements

The z/OS Communication Server IP CICS socket interface and listener use the latest version of the CICS/TS macros. This version of the macros provides load module addressability relief in IP CICS socket load modules and the ability to run on all available releases of CICS/TS.

There are no tasks to enable this function; it is automatically enabled.

Availability and business resilience

z/OS V1R11 Communications Server includes enhancements to availability and business resilience in the following areas:

- "Improved responsiveness to storage shortage conditions"
- "Disable moving DVIPA as source IP address" on page 68
- "Support for enhanced WLM routing algorithms" on page 68

Improved responsiveness to storage shortage conditions

In z/OS V1R11 Communications Server, TCP/IP and OMPROUTE processing is improved to do the following:

- Provide CSM extended common service area (ECSA) storage relief in response to excessive storage on the send queue for a TCP connection
- Issue messages to syslogd when excessive or old data is accumulating on the receive or send queue for a TCP connection
- Increase the likelihood that OMPROUTE will continue to function through a temporary storage shortage, such as experiencing CSM ECSA or CSM data space conditions or reaching the TCP/IP defined limits for ECSA or private storage

In addition, z/OS Communications Server inbound processing for OSA-Express in QDIO mode and HiperSockets devices monitors the amount of ECSA storage buffered on the inbound data path. When ECSA storage usage for a particular device is excessive or when ECSA limits become constrained or critical, packets might be intentionally discarded to minimize impacts to system performance and system integrity.

Restriction: Packets will only be intentionally discarded for OSA-Express in QDIO mode and HiperSockets devices.

Incompatibility: If the CIA VTAM internal trace option is not enabled, discarded packets are not traced.

Using the improved responsiveness to storage shortage conditions

There are no tasks to provide CSM ECSA storage relief, to increase the likelihood that OMPROUTE will continue to function through a temporary storage shortage, or to use the improvements associated with discarding packets. Those functions are automatically enabled. The tasks in Table 54 are optional.

Table 54. Improved responsiveness to storage shortage conditions

Task	Procedure	Reference
Enable the issuing of messages to syslogd when excessive or old data is accumulating on the receive or send queue for a TCP connection.	Configure and start syslogd and TRMD.	Configuring the syslog daemon (syslogd) and TRMD in *z/OS Communications Server: IP Configuration Guide*

Table 54. Improved responsiveness to storage shortage conditions (continued)

Task	Procedure	Reference
Diagnose storage problems with TCP applications.	Complete the storage problem steps described in *z/OS Communications Server: IP Diagnosis Guide*. Look for the messages that are issued when excessive or old data is accumulating on a TCP receive or send queue.	Diagnosing storage abends and storage growth in *z/OS Communications Server: IP Diagnosis Guide*

Disable moving DVIPA as source IP address

The TCPSTACKSOURCEVIPA function is enhanced in z/OS V1R11 Communications Server to prevent the stack from using dynamic virtual IP addresses (DVIPAs) in MOVING state as source IP addresses. New TCP outbound connections that are established after the DVIPA has transitioned to the MOVING state no longer use the DVIPA as a source IP address. This enables DVIPAs in the MOVING state to return to their original state in a timely manner.

There are no tasks to enable this function; it is automatically enabled.

Support for enhanced WLM routing algorithms

z/OS V1R11 Communications Server enhances server-specific workload manager (WLM) recommendations that are used by the sysplex distributor to balance workload when DISTMETHOD SERVERWLM is configured on the VIPADISTRIBUTE statement. Two new configuration parameters enable WLM to do the following:

- Direct more workload targeted for zIIP or zAAP specialty processors to systems that have these more affordable processor cycles available, thereby reducing the overall cost of running those workloads
- Consider the different importance levels of displaceable capacity when determining server-specific recommendations

Restriction: The new configuration parameters can be used by WLM for server-specific recommendations only when all systems in the sysplex are V1R11 or later. In a mixed-release environment, the new crossover costs and importance level weighting parameters are ignored by WLM when it determines a server-specific weight.

Dependency: At a minimum, an IBM System z® Integrated Information Processor (IBM zIIP) or IBM System z Application Assist Processor (zAAP) is required for workloads that are targeted to a zIIP or zAAP

Using the support for enhanced WLM routing algorithms

If you want to use this function, perform the appropriate tasks in Table 55 on page 69.

Table 55. Support for enhanced WLM routing algorithms

Task	Procedure	Reference
Specify crossover costs for running a server's zIIP or zAAP targeted workload on a conventional processor. These costs are used by WLM when it determines a server-specific recommendation.	Perform the following steps: 1. Add or change the PROCXCOST parameter on a VIPADISTRIBUTE statement that has a DISTMETHOD parameter that has a value of SERVERWLM. 2. Issue a VARY TCPIP,,OBEYFILE command for the modified profile.	VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*
Specify how aggressively WLM should favor displaceable capacity at lower importance levels over capacity at higher importance levels when it determines a server-specific recommendation.	Perform the following steps: 1. Add or change the ILWEIGHTING parameter on a VIPADISTRIBUTE statement that has a DISTMETHOD parameter that has a value of SERVERWLM. 2. Issue a VARY TCPIP,,OBEYFILE command for the modified profile.	VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*
Verify the configured crossover costs for running workloads targeted to zIIP or zAAP.	Use the Netstat VIPADCFG/-F DETAIL command to determine the configured crossover costs that will be passed to WLM by sysplex distributor.	Netstat VIPADCFG/-F report in *z/OS Communications Server: IP System Administrator's Commands*
Verify the configured ILWEIGHTING value.	Use the Netstat VIPADCFG/-F DETAIL command to determine the configured ILWEIGHTING value that will be passed to WLM by sysplex distributor.	Netstat VIPADCFG/-F report in *z/OS Communications Server: IP System Administrator's Commands*

Scalability, performance, constraint relief, and accelerators

z/OS V1R11 Communications Server includes enhancements to scalability, performance, constraint relief, and accelerators in the following areas:

- "accept_and_receive API enhancements"
- "TCP/IP support for system z10 hardware instrumentation" on page 70
- "TCP/IP pathlength improvements" on page 70
- "TCP throughput improvements for high-latency networks" on page 71
- "Virtual storage constraint relief" on page 71
- "NSS private key and certificate services for XML appliances" on page 72
- "Enterprise Extender IPSec performance improvements" on page 72
- "Resolver DNS cache" on page 73
- "Sysplex autonomics improvements for FRCA" on page 74
- "QDIO routing accelerator" on page 74
- "Sysplex distributor enhancements" on page 75
- "OSA-Express3 optimized latency mode" on page 78

accept_and_receive API enhancements

The accept_and_recv socket API enables z/OS applications and middleware to process short-lived client TCP connections more efficiently by combining the functions of multiple socket calls into one call. Although the accept_and_recv API has been available for several releases, z/OS V1R11 Communications Server contains significant enhancements:

- accept_and_recv socket calls can be issued asynchronously using the UNIX System Services Async I/O (BPX1AIO or BPX4AIO) callable services.
- The accept_and_recv processing is implemented natively in the Communications Server TCP/IP protocol stack. This reduces the overhead associated with communications between the UNIX System Services layer and TCP/IP.
- Incoming TCP connections that might incur delays in receiving data are processed more efficiently. The accept_and_recv processing can now logically separate these connections from connections that are functioning optimally so that they do not impact the performance of accept_and_recv API requests.

There are no tasks to enable this function; it is automatically enabled.

Restrictions:

- The accept_and_receive API does not support the msg_waitall option.
- Asynchronous accept_and_recv() calls cannot be mixed with asynchronous accept() calls.

TCP/IP support for system z10 hardware instrumentation

In z/OS V1R11 Communications Server, TCP/IP uses the z/OS MVS CSVDYLPA service to load its load modules. Using CSVDYLPA gives the z/OS MVS Contents Supervisor awareness of the location and attributes of z/OS Communication Server load modules and entry points. Vendor utility functions that intend to map z/OS Communication Server code can use the z/OS MVS services CSVQUERY or CSVINFO to obtain the location of z/OS Communications Server load modules and entry points.

There are no tasks for this function; CSVDYLPA is used unconditionally.

TCP/IP pathlength improvements

In z/OS V1R11 Communications Server, the TCP layer is updated to detect and react transparently to two common sockets programming errors:

- Traffic stalls caused by Nagle algorithms and delayed TCP acknowledgements
- Deadlock caused by insufficient TCP receive buffer size

Traffic stalls caused by Nagle algorithms and delayed TCP acknowledgements

Certain transactional workloads tend to perform back-to-back socket send() calls that contain small amounts of data, with no intervening inbound activity. If the application has not disabled the Nagle algorithm by means of the TCP_NODELAY SetSockOpt call, the second send() call will queue until the data of the first send call() is acknowledged by the other side of the TCP connection. A problem can arise because most TCP stacks try to acknowledge every other packet. When the Nagle algorithm in the side of the TCP connection that sent the packet allows only a single packet to flow, the receiver becomes dependent upon its Delay Ack Timer (typically 200 milliseconds) before an ACK to the first segment is generated. The result is that traffic slows to fewer than five round trips per second. In z/OS V1R11 Communications Server, the send-side Nagle algorithm avoids such traffic stalls caused by delayed TCP acknowledgements from the receiver side of the TCP connection.

Deadlock caused by insufficient TCP receive buffer size

The *msg_waitall* flag on the read() call instructs the TCP layer not to post completion of the socket read() call until all of the requested data is present. This flag makes receive processing very efficient because it minimizes the number of

socket receive API crossings. Using this flag can cause a deadlock to occur if an insufficient TCP receive buffer size has been configured. The socket read() call is never posted in such a case. This scenario occurs when an application issues a *msg_waitall* socket read() call with a specific number of bytes, but configures a TCP receive buffer size of fewer bytes. In this case, TCP flow control stops the data flow before the full number of bytes of data can accumulate. z/OS V1R11 Communications Server detects this deadlock situation and it transparently increases the TCP receive buffer size so that the connection flows until the full number of bytes is present.

There are no tasks for TCP/IP pathlength improvements; they are automatically enabled.

TCP throughput improvements for high-latency networks

z/OS V1R11 Communications Server improves performance for inbound streaming TCP connections over networks with large bandwidth and high latency by automatically tuning the ideal window size for such TCP connections.

Restriction: This function does not take effect for applications that request a TCP receive buffer size smaller than 64 K on the SO_RCVBUF socket option on SETSOCKOPT() call. Also, if the TCPRCVBUFRSIZE value is less than 64 K, then this function does not take effect for applications that do not use the SO_RCVBUF socket option on the SETSOCKOPT() call.

Using TCP throughput improvements for high-latency networks

If you want to use this function, perform the appropriate tasks in Table 56.

Table 56. TCP throughput improvements for high-latency networks

Task	Procedure	Reference
Enable the TCP stack to automatically tune the ideal window size for inbound streaming TCP connections over networks that have large bandwidth and high latency.	Specify a TCP receive buffer size value of at least 64 K on the TCPRCVBUFRSIZE parameter of the TCPCONFIG statement.	TCPCONFIG in *z/OS Communications Server: IP Configuration Reference*
Determine whether the stack is automatically tuning the ideal window size for a TCP connection.	Issue the Netstat ALL/-A command.	Netstat ALL/-A report in *z/OS Communications Server: IP System Administrator's Commands*

Virtual storage constraint relief

z/OS V1R11 Communications Server moves some data areas that map socket connections from ECSA to storage that is above the 2-gigabyte threshold. This change can provide additional common storage (ECSA) constraint relief; the ECSA storage reduction is directly proportional to the number of open sockets.

Using the virtual storage constraint relief

There are no tasks to enable this function; it is automatically enabled. To see the storage usage, perform the task in Table 57 on page 72.

Table 57. Virtual storage constraint relief

Task	Procedure	Reference
Display the ECSA and 64-bit common TCP/IP storage usage information.	Specify the DISPLAY TCPIP, *procname*,STOR command.	DISPLAY TCPIP,,STOR in *z/OS Communications Server: IP System Administrator's Commands*

NSS private key and certificate services for XML appliances

z/OS V1R11 Communications Server enhances network security services (NSS) to improve XML appliance security as a logical extension of z/OS security. Two new services are added to the XMLAppliance discipline, which is supported by the NSS server:

- The XMLAppliance certificate service provides certificate management operations.
- The XMLAppliance private key service enables retrieval of private keys that are not protected by ICSF (Integrated Cryptographic Service Facility) from certificates on the configured SAF key ring and performs RSA signature creation and RSA decryption using ICSF-protected private keys.

Using NSS private key and certificate services for XML appliances

If you want to use this function, perform the appropriate tasks in Table 58.

Table 58. NSS private key and certificate services for XML appliances

Task	Procedure	Reference
Configure the NSS server to enable the XMLAppliance discipline.	Add the Discipline parameter with the XMLAppliance keyword in the NssConfig statement in the NSS configuration file.	Preparing to provide network security services in *z/OS Communications Server: IP Configuration Guide*
Enable XMLAppliance clients to access network security services.	Add corresponding SERVAUTH definitions to SAF-compliant security product profiles to enable clients to use the XMLAppliance certificate and private key services.	Preparing to provide network security services in *z/OS Communications Server: IP Configuration Guide*
Enable XMLAppliance clients to access appropriate certificates and private keys.	Add corresponding SERVAUTH definitions to SAF-compliant security product profiles to enable clients to access certificates and private keys.	Preparing to provide network security services in *z/OS Communications Server: IP Configuration Guide*
Monitor different types of NSS clients that are currently connected to the NSS server.	Use the **nssctl -d** command.	nssctl in *z/OS Communications Server: IP System Administrator's Commands*
Enable ICSF when using XMLAppliance private key service.	Install and initialize ICSF.	Steps for Installation and initialization in *z/OS Cryptographic Services ICSF System Programmer's Guide*

Enterprise Extender IPSec performance improvements

z/OS V1R11 Communications Server improves performance when IP security is used to protect Enterprise Extender (EE) connections. IP processing now optimizes the EE path length when EE is protected by IPSec, as well as makes better use of zIIP processors for systems that are configured to use zIIPs.

No tasks are necessary; these enhancements are automatically enabled.

Resolver DNS cache

In z/OS V1R11 Communications Server, the resolver can use system-wide caching of Domain Name System (DNS) responses. The system resolver cache can be used to eliminate redundant network flows to DNS servers, which can provide significant performance improvements for z/OS workloads that perform repetitive resolver queries. The resolver cache is enabled by default and is shared across the entire z/OS system image. If you are currently running a caching-only DNS name server, you might be able to use the resolver DNS cache instead; the resolver DNS cache provides the same function with better system performance.

Using the resolver DNS cache

You do not have to perform any steps to enable the resolver DNS caching function; it is automatically enabled. The tasks in Table 59 are optional.

Table 59. Resolver DNS cache

Task	Procedure	Reference
Determine whether caching is in effect on a system-wide basis.	Issue the MODIFY RESOLVER,DISPLAY command and look for the EZZ9304I CACHE message.	MODIFY command -- Resolver address space in *z/OS Communications Server: IP System Administrator's Commands*
Determine whether caching is in effect for a specific application or resolver query.	Perform the following steps: 1. Enable the trace resolver function. 2. Start the application. 3. Issue the resolver query. 4. Examine the trace resolver res_init( ) information to determine whether the Cache or NoCache value is specified.	TRACE RESOLVER in *z/OS Communications Server: IP Diagnosis Guide*
Disable resolver DNS caching on a system-wide or application basis.	To disable system-wide caching, perform the following steps: 1. Specify the NOCACHE resolver setup statement in the resolver setup file data set. 2. Issue the MODIFY RESOLVER,REFRESH,SETUP=<*resolver setup file name*> command. To disable caching on an application basis, perform the following steps: 1. Specify the NOCACHE statement in the TCPIP.DATA file used by this application. 2. Issue the MODIFY RESOLVER,REFRESH command or restart the application.	See the following topics in *z/OS Communications Server: IP Configuration Reference*: • CACHE NOCACHE statements • NOCACHE statement (TCPIP.DATA statement)

Table 59. Resolver DNS cache (continued)

Task	Procedure	Reference
Re-enable resolver DNS caching on a system-wide or application basis.	To re-enable system-wide caching, perform the following steps: 1. Specify the CACHE resolver setup statement in the resolver setup file data set, or remove the NOCACHE resolver setup statement from the resolver setup file data set. 2. Issue the MODIFY RESOLVER,REFRESH,SETUP=<*resolver setup file name*> command. To re-enable caching on an application basis, perform the following steps: 1. Remove the NOCACHE statement in the TCPIP.DATA file used by this application. 2. Issue the MODIFY RESOLVER,REFRESH command or restart the application.	See the following topics in *z/OS Communications Server: IP Configuration Reference*: • CACHE NOCACHE statements • NOCACHE statement (TCPIP.DATA statement)
Increase the maximum amount of storage that can be allocated for the resolver DNS cache.	Perform the following steps: 1. Specify the CACHESIZE resolver setup statement in the resolver setup file data set. 2. Issue the MODIFY RESOLVER,REFRESH,SETUP=<*resolver setup file name*> command.	CACHESIZE statement in *z/OS Communications Server: IP Configuration Reference*
Delete all the resolver cache data.	Issue the MODIFY RESOLVER,FLUSH,ALL command.	MODIFY command -- Resolver address space in *z/OS Communications Server: IP System Administrator's Commands*
Display information about the resolver cache.	Use the Netstat RESCache/-q command to display resolver cache statistics and detailed cache entry information.	Netstat RESCache/-q report in *z/OS Communications Server: IP System Administrator's Commands*

Sysplex autonomics improvements for FRCA

z/OS V1R11 Communications Server improves the accuracy of the server efficiency factor (SEF) for server applications using the Fast Response Cache Accelerator (FRCA) function with persistent HTTP connections. The SEF is one of the measures of the health of a particular server on a particular target stack. The higher the value, the healthier the application is. It generally measures how well a server application is processing established connections on its backlog queue.

There are no tasks for this function; it is automatically enabled.

QDIO routing accelerator

In z/OS V1R11 Communications Server, the QDIO routing accelerator function provides accelerated forwarding at the DLC layer for the following inbound packets:

- Inbound packets that are routed over HiperSockets and that are being forwarded outbound over OSA-Express QDIO or HiperSockets
- Inbound packets that are routed over OSA-Express QDIO and that are being forwarded outbound over OSA-Express QDIO or HiperSockets

Similar to HiperSockets accelerator, QDIO routing accelerator can improve latency and decrease CPU consumption for all accelerated traffic when routing forwarded

traffic early during inbound processing. The QDIO routing accelerator function also provides accelerated forwarding of packets that the sysplex distributor forwards to a target stack when the packets are flowing over one of the above inbound and outbound DLC combinations.

Restrictions:

- The QDIO accelerator is limited to IPv4.
- The QDIO accelerator cannot be enabled if IP security is enabled on the stack.
- If IP forwarding is disabled on the stack, then the QDIO accelerator is limited to sysplex distributor forwarding.
- When the outbound interface is HiperSockets, packets from the sysplex distributor to the target are not accelerated with the VIPAROUTE destination.

Incompatibilities: Packets that are accelerated by the QDIO accelerator are not traced by the packet trace function on the forwarding stack; however, you can use the OSA-Express network traffic analyzer (OSAENTA) function to trace the packets that are accelerated to or from OSA-Express QDIO interfaces. For more information about OSAENTA, see OSA-Express network traffic analyzer trace in *z/OS Communications Server: IP Configuration Guide*.

Using the QDIO routing accelerator

If you want to use this function, perform the appropriate tasks in Table 60.

Table 60. QDIO routing accelerator

Task	Procedure	Reference
Enable the QDIO accelerator function to provide accelerated forwarding of packets.	Specify the QDIOACCELERATOR parameter on the IPCONFIG statement in the TCP/IP profile.	IPCONFIG statement in *z/OS Communications Server: IP Configuration Reference*
Display whether the QDIO accelerator is enabled.	Issue the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*
Display the QDIO accelerator routes.	Issue the Netstat ROUTe/-r command with the QDIOACCEL parameter.	Netstat ROUTe/-r report in *z/OS Communications Server: IP System Administrator's Commands*
Display whether a sysplex distributor connection is eligible for acceleration.	Issue the Netstat VCRT/-V command with the DETAIL modifier.	Netstat VCRT/-V report in *z/OS Communications Server: IP System Administrator's Commands*
Display information about the number of packets and bytes that are accelerated after they are received over a specific interface.	Initiate VTAM tuning statistics for the OSA-Express QDIO or HiperSockets interface.	MODIFY TNSTAT command in *z/OS Communications Server: SNA Operation*
See information similar to packet trace information for packets that are accelerated either from or to an OSA-Express QDIO interface.	Use the OSAENTA function.	OSA-Express network traffic analyzer trace in *z/OS Communications Server: IP Configuration Guide*

Sysplex distributor enhancements

z/OS V1R11 Communications Server enhances sysplex distributor in the following areas:

- "Sysplex distributor connection routing accelerator" on page 76

- "Sysplex distributor optimization for multi-tier z/OS workloads"
- "Sysplex distributor support for DataPower" on page 77

Sysplex distributor connection routing accelerator

In z/OS V1R11 Communications Server, the QDIO accelerator provides accelerated forwarding of packets that the sysplex distributor forwards to a target stack when the packets are flowing over one of the following inbound and outbound DLC combinations:

- Inbound packets that are routed over HiperSockets and that are being forwarded outbound over OSA-Express QDIO or HiperSockets
- Inbound packets that are routed over OSA-Express QDIO and that are being forwarded outbound over OSA-Express QDIO or HiperSockets

Similar to HiperSockets accelerator, QDIO routing accelerator can improve latency and decrease CPU consumption for all accelerated traffic when routing forwarded traffic early during inbound processing.

See "QDIO routing accelerator" on page 74 for more information about QDIO acceleration.

Using the sysplex distributor connection routing accelerator: If you want to use this function, perform the appropriate tasks in Table 61.

Table 61. Sysplex distributor connection routing accelerator

Task	Procedure	Reference
Enable the QDIO accelerator function to provide accelerated forwarding of packets.	Specify the QDIOACCELERATOR parameter on the IPCONFIG statement in the TCP/IP profile.	IPCONFIG statement in *z/OS Communications Server: IP Configuration Reference*
Display whether the QDIO accelerator is enabled.	Issue the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*
Display whether a sysplex distributor connection is eligible for acceleration.	Issue the Netstat VCRT/-V command with the DETAIL modifier.	Netstat VCRT/-V report in *z/OS Communications Server: IP System Administrator's Commands*
Display information about the number of packets and bytes that are accelerated after being received over a specific interface.	Initiate VTAM tuning statistics for the OSA-Express QDIO or HiperSockets interface.	MODIFY TNSTAT command in *z/OS Communications Server: SNA Operation*
See information similar to packet trace information for packets that are accelerated either from or to an OSA-Express QDIO interface.	Use the OSAENTA function.	OSA-Express network traffic analyzer trace in *z/OS Communications Server: IP Configuration Guide*

Sysplex distributor optimization for multi-tier z/OS workloads

Prior to z/OS V1R11 Communications Server, you could configure sysplex distributor with OPTLOCAL to optimize connections when both connection endpoints potentially reside on the same TCP/IP stack within the sysplex. This feature can be useful in environments where multi-tier server applications are all located within the same z/OS system images in a single sysplex. In this type of environment, OPTLOCAL is deployed on the tier 2 sysplex distributor to optimize the connections between tier 1 and tier 2 server applications.

z/OS V1R11 allows a further optimization if sysplex distributor is also being used as the load balancer for the tier 1 server applications. This optimization allows the tier 1 sysplex distributor to have visibility into both tiers of the z/OS server applications on a given system when making a load balancing decision on an incoming tier 1 connection request. When using WLM based recommendations, this optimization allows sysplex distributor to compute a composite WLM weight for each system that includes the capacity, performance, and health characteristics of both the tier 1 server applications and the tier 2 server applications.

For a step-by-step description of how to use this function, see the information about sysplex distribution optimization for multi-tier z/OS workloads in *z/OS Communications Server: IP Configuration Guide*.

Restriction: All TCP/IP stacks that participate in the sysplex distribution as distributing, backup, or target stacks must be at V1R11 or later.

Sysplex distributor support for DataPower

The sysplex distributor feature of Communications Server provides workload balancing capabilities for TCP applications in a z/OS sysplex environment. These capabilities can significantly enhance the availability, performance, and scalability characteristics of z/OS TCP/IP-based applications. In z/OS V1R11 Communications Server, sysplex distributor is enhanced to provide similar workload balancing capabilities for IBM WebSphere DataPower appliances. DataPower appliances are often deployed as a front-end processing tier to z/OS applications, which provides for transparent web services enablement of z/OS applications or accelerated and more efficient handling of web services security protocols, XML schema validation, and additional functions. In many of these environments, multiple DataPower instances are deployed in a cluster to provide higher availability and scalability, requiring an external, network-based load balancer to load balance incoming requests across the DataPower appliance instances.

When the DataPower tier finishes handling a request, it typically routes a request to a tier 2 application that is hosted within the z/OS environment, such as a CICS TM, IMS TM, or WebSphere application. These tier 2 requests might also require load balancing, especially when the applications are deployed in a sysplex environment. Prior to z/OS V1R11 Communications Server, sysplex distributor could be used to load balance the tier 2 requests into the z/OS sysplex. With this V1R11 enhancement, you can use sysplex distributor to load balance requests to both the DataPower and z/OS tiers, eliminating the need for deploying an external, network-based load balancer for the DataPower tier.

This enhancement also includes new support in the IBM WebSphere DataPower appliance, which enables sysplex distributor to optimize the load balancing support in several ways:

- Routing is optimized so that outbound traffic (from the tier 1 DataPower target server towards the client) does not need to traverse the sysplex distributor.
- Connection information provided by the DataPower appliances allows nondisruptive tier 1 takeover of existing connections between clients and DataPower targets.
- CPU usage information provided by the DataPower appliance allows sysplex distributor to optimize its load balancing decisions.

For more information and for step-by-step lists of tasks describing how to use sysplex distribution with DataPower, see the information about sysplex distribution with DataPower in *z/OS Communications Server: IP Configuration Guide*.

Restriction: All TCP/IP stacks that participate in the sysplex distributor support with DataPower must be V1R11 or later.

Coexistence requirements: An IBM WebSphere DataPower appliance with support for these optimizations is required in this environment.

OSA-Express3 optimized latency mode

z/OS V1R11 Communications Server improves performance for workloads that have demanding latency requirements because it provides a way for an OSA-Express3 device to run in optimized latency mode. Optimized latency mode optimizes interrupt processing for both inbound and outbound data. When an OSA-Express3 device is operating in optimized latency mode, latency is decreased and throughput is increased, particularly for interactive, non-streaming workloads.

Restriction: The number of concurrent network interfaces that can share an OSA-Express3 device is limited. No more than four concurrent network interfaces can share an OSA-Express port when one or more of those network interfaces are operating in optimized latency mode. No more than eight concurrent network interfaces can share an OSA-Express channel path identifier (CHPID) when one or more of those network interfaces are operating in optimized latency mode.

Incompatibilities:

- Traffic directed to OSA-Express3 write priority queue 4 will not benefit from optimized latency mode for outbound interrupt optimization.
- Traffic that is either inbound over or being forwarded to an OSA-Express3 device configured in optimized latency mode is not eligible for the accelerated routing function provided by HiperSockets Accelerator and QDIO Accelerator.
- Optimized latency mode can be configured only for an OSA-Express3 device that is configured with an INTERFACE statement, not with DEVICE and LINK statements.
- The optimized latency mode function targets a specific z/OS environment that has high-volume interactive workloads. Although optimized latency mode can compensate for some mixing of workloads, an excessive amount of high volume, streaming workloads, such as bulk data or file transfer, can result in higher CPU consumption.

Dependencies: This function is limited to OSA-Express3 ethernet features in QDIO mode running on an IBM System z10. See the 2097DEVICE and the 2098DEVICE Preventive Service Planning (PSP) buckets for further information.

Using the OSA-Express3 optimized latency mode

If you want to use this function, perform the tasks in Table 62.

Table 62. OSA-Express3 optimized latency mode

Task	Procedure	Reference
Enable an OSA-Express3 device for optimized latency mode.	Specify the OLM parameter on the INTERFACE statement in the TCP/IP profile.	INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces in *z/OS Communications Server: IP Configuration Reference*
Direct traffic to OSA-Express3 write priority queues 1, 2, or 3.	Specify the WLMPRIORITYQ parameter on the GLOBALCONFIG statement in the TCP/IP profile.	GLOBALCONFIG in *z/OS Communications Server: IP Configuration Reference*
Display OSA-Express3 performance options.	Issue the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d report in *z/OS Communications Server: IP System Administrator's Commands*
Determine the effectiveness of optimizing interrupts by using optimized latency mode.	Issue the MODIFY TNSTAT command to display the tuning statistics for an OSA-Express3 device.	• MODIFY TNSTAT command in *z/OS Communications Server: SNA Operation* • Message IST1230I in *z/OS Communications Server: SNA Messages*

Security

z/OS V1R11 Communications Server includes enhancements to security in the following areas:

- "IPSec enhancements"
- "AT-TLS enhancements" on page 80

IPSec enhancements

The Internet Key Exchange (IKE) daemon's retransmission scheme better conforms to RFC 2408. Rather than using fixed intervals for IKE message retransmission, the daemon uses a geometrically increasing retransmission interval. Some fine-grained attributes are reported in the **ipsec** command reports as well as in the Network Management Interface (NMI) and System Management Facility (SMF) records.

Restriction: The existing DataRetries, DataWait, KeyRetries, and KeyWait parameters in the IKED configuration file are no longer honored. Instead, the new IkeRetries and IkeInitWait parameters control message retransmission for all IKE messages.

Using the IPSec enhancements

No explicit tasks are required to use the z/OS V1R11 Communications Server IPSec enhancements. If you use the Configuration Assistant to generate the IKED configuration file, you need to obtain the V1R11 Configuration Assistant. The files generated with the V1R11 version of the tool use the new defaults. You can optionally change these settings in the Advanced IKE Daemon Settings dialog box under the **IKE Daemon Settings** tab under the IPSec perspective for the z/OS image.

If you manually edit your IKED configuration file, the new IkeRetries and IkeInitWait parameters both have default values, and because of the nature of the geometrically increasing intervals, the same default value should be sufficient for all IKE partners. However, if you have a specific need to control the initial retransmission interval or number of retries, code the corresponding IkeInitWait and IkeRetries parameters in the IKED configuration file and then apply the new configuration by issuing a MODIFY IKED,REFRESH command.

Optionally, you can also remove any DataRetries, DataWait, KeyRetries, and KeyWait parameters from the IKED configuration file because they are no longer honored.

AT-TLS enhancements

In z/OS V1R11 Communications Server, AT-TLS supports the System SSL functions that have been added since z/OS V1R7. This includes support for the following:

- The TLSv1.1 protocol
- RFC 3280 for certificate validation
- FIPS 140-2
- PKCS #11 Token names for Keyring
- Negotiation and use of a truncated Hash Message Authentication Code (HMAC)
- Negotiation and use of a maximum SSL fragment size
- Negotiation and use of handshake server name indication
- Setting the CRL LDAP server access security level

IBM Configuration Assistant for z/OS is enhanced to define use of these new AT-TLS functions.

Restrictions:

- Applications using the Pascal application programming interface are not supported by AT-TLS. The new functions are not supported for Pascal applications.
- To enable FIPS 140-2 support, Security Level 3 FMID (JCPT3B1) must be installed.

Using the AT-TLS enhancements

If you want to use this function, perform the task in Table 63.

Table 63. AT-TLS enhancements

Task	Procedure	Reference
Define the new AT-TLS statements in the Policy Agent configuration files.	Specify the new AT-TLS statements in the configuration files that are identified with the CommonTTLSConfig and TTLSConfig statements by using one of the following methods: • Use the z/OS Network Security Configuration Assistant. • Code the required statements directly into an HFS file or MVS data set.	• Application Transparent Transport Layer Security data protection in *z/OS Communications Server: IP Configuration Guide* • AT-TLS policy statements in *z/OS Communications Server: IP Configuration Reference* • IBM Configuration Assistant for z/OS Communications Server online helps

Table 63. AT-TLS enhancements (continued)

Task	Procedure	Reference
If FIPS 140-2 is enabled, configure System SSL for FIPS 140-2 support.	Complete the steps described in *z/OS Cryptographic Services System SSL Programming* to set up System SSL to run in FIPS-mode.	*z/OS Cryptographic Services System SSL Programming*

Simplification and consumability

z/OS V1R11 Communications Server includes enhancements to simplification and consumability in the following areas:

- "Configuration Assistant enhancements"
- "syslogd enhancements" on page 82
- "syslogd browser and search facilities" on page 82
- "Policy infrastructure management enhancements" on page 83
- "MVS console support for select TCP/IP commands" on page 85
- "IBM Health Checker for z/OS DNS server check" on page 85

Configuration Assistant enhancements

The IBM Configuration Assistant for z/OS Communications Server V1R11 (Configuration Assistant) simplifies the installation and setup of policies. In addition to installing policy files, the Configuration Assistant guides the administrator through all of the tasks that are necessary to get the Communications Server function (such as IPSec) active and running on the z/OS system. These tasks include everything from setting up RACF security to starting Policy Agent and other daemons that might be used by the function.

The following list identifies the new Configuration Assistant functions:

- Configure the Policy Agent configuration file
- Configure the Defense Manager Daemon (DMD)
- Configure the base location
- Customize EBCDIC codepage support
- Set up Policy Agent tasks
- Install an **all files** option
- Notify the administrator when configuration data is changed

Using the Configuration Assistant enhancements

If you want to use the Configuration Assistant enhancements, perform the task in Table 64.

Table 64. Configuration Assistant enhancements

Task	Procedure	Reference
Use the Configuration Assistant.	Install the IBM Configuration Assistant for z/OS V1R11 and refer to the help topics.	You can download the GUI from the z/OS Communications Server product support Web page. Invoke the Configuration Assistant Help System.

syslogd enhancements

In z/OS V1R11 Communications Server, the internal structure of syslog daemon (syslogd) provides more efficient processing of log messages. The syslogd job name matches the name of the cataloged procedure, and a set of operator commands starts, stops, and controls the daemon. The syslog daemon also performs automatic archival of z/OS UNIX files, based on configurable options.

Using the syslogd enhancements

If you want to use the syslogd enhancements, perform the tasks in Table 65.

Table 65. syslogd enhancements

Task	Procedure	Reference
Use operator commands to control the syslog daemon.	Perform the following steps: 1. Issue the STOP command to stop the syslog daemon. The effect is the same as sending a SIGTERM signal. 2. Issue the MODIFY *procname*,RESTART command to restart the syslog daemon. The effect is the same as sending a SIGHUP signal.	STOP command and MODIFY command: Syslog Daemon in *z/OS Communications Server: IP System Administrator's Commands*
Configure the syslog daemon to perform automatic archival of eligible z/OS UNIX files at a specific local time of day or based on a file-system threshold.	Specify the following configuration statements or parameters in the syslogd configuration file: • ArchiveTimeOfDay statement to specify a specific local time of day for archiving • ArchiveThreshold and ArchiveCheckInterval statements to specify the threshold archiving for the z/OS UNIX file system • BeginArchiveParms statements to specify archive details for eligible z/OS UNIX files • -N or -X parameter on syslogd rules that have a z/OS UNIX file destination. The -N and -X parameters specify archive details for the file or that the file should be reinitialized.	• Configuring the syslog daemon (syslogd) in *z/OS Communications Server: IP Configuration Guide* • Syslog daemon in *z/OS Communications Server: IP Configuration Reference*
Display z/OS UNIX file system usage data for configured syslogd z/OS UNIX files.	Issue the MODIFY *procname*,DISPLAY,ARCHIVE command.	MODIFY command: Syslog daemon in *z/OS Communications Server: IP System Administrator's Commands*
Perform an on-demand archive of all eligible syslogd z/OS UNIX files.	Issue the MODIFY *procname*,ARCHIVE command.	MODIFY command: Syslog daemon in *z/OS Communications Server: IP System Administrator's Commands*

syslogd browser and search facilities

In z/OS V1R11 Communications Server, an ISPF-based syslog daemon browser application is available. The browser supports browsing and searching active syslogd files (the files to which syslogd currently writes) and syslogd archive data sets that were created using the new syslogd archival function.

Using the syslogd browser and search facilities

If you want to use the syslogd browser and search facilities, see Table 66.

Table 66. syslogd browser and search facilities

Task	Procedure	Reference
Browse or search active syslogd files and archive data sets.	Make the z/OS V1R11 Communications Server ISPF libraries available in TSO.	Syslog daemon in *z/OS Communications Server: IP Configuration Reference*

Policy infrastructure management enhancements

In z/OS V1R11 Communications Server, the Policy Agent provides monitoring and automatic start and restart for the following set of related applications:

- Defense manager daemon (DMD)
- Internet key exchange daemon (IKED)
- Network security services daemon (NSSD)
- syslog daemon (syslogd)
- Traffic regulation management daemon (TRMD)

This function is similar to the AUTOLOG function in the TCP/IP stack, but it does not require the application to maintain a listening socket. This function provides simpler management and operations for a set of applications that are associated with the policy infrastructure.

A variety of EBCDIC code pages are supported for the configuration files and policy definition files for the following applications:

- Policy Agent
- syslogd
- IKED
- NSSD
- DMD

You can specify as a start option the TCP/IP stack name that the TRMD uses. You can still use the resolver configuration file to specify the stack name.

Using the policy infrastructure management enhancements

If you want to use the policy infrastructure management enhancements, perform the tasks in Table 67.

Table 67. Policy infrastructure management enhancements

Task	Procedure	Reference
Determine the set of applications to be monitored by the Policy Agent.	Examine your z/OS Communications Server environment to determine which of the following daemons are currently used and which daemons you want Policy Agent to monitor: • DMD • IKED • NSSD • syslogd • TRMD	Configuring Policy Agent to automatically monitor applications in *z/OS Communications Server: IP Configuration Guide*

Table 67. Policy infrastructure management enhancements (continued)

Task	Procedure	Reference
Configure the Policy Agent to monitor the target set of applications.	Specify the following configuration statements in the Policy Agent main configuration file: • AutoMonitorApps statement to specify the applications to be monitored, as well as application-specific parameters • AutoMonitorParms statement to specify global monitoring parameters	• Configuring Policy Agent to automatically monitor applications in *z/OS Communications Server: IP Configuration Guide* • AutoMonitorApps statement and AutoMonitorParms statement in *z/OS Communications Server: IP Configuration Reference*
Optionally, manage the target set of applications using Policy Agent MODIFY commands.	Do one or more of the following: • Issue the MODIFY *procname*,MON,START,*application* command to start a monitored application that failed to start automatically. • Issue the MODIFY *procname*,MON,STOP,*application* command to stop a monitored application and to also stop monitoring the application. • Issue the MODIFY *procname*,MON,RESTART,*application* command to stop and restart a monitored application. • Issue the MODIFY *procname*,MON,DISPLAY command to display the status of monitored applications.	• Configuring Policy Agent to automatically monitor applications in *z/OS Communications Server: IP Configuration Guide* • MODIFY command: Policy Agent in *z/OS Communications Server: IP System Administrator's Commands*
Specify the EBCDIC code page to be used for reading the Policy Agent configuration files and policy definition files.	Configure the CODEPAGE configuration statement in the main Policy Agent configuration file.	CODEPAGE statement in *z/OS Communications Server: IP Configuration Reference*
Specify the EBCDIC code page to be used for reading the configuration files for policy-related applications.	Specify the appropriate code page environment variable for the following applications: • syslogd: SYSLOGD_CODEPAGE • IKED: IKED_CODEPAGE • NSSD: NSSD_CODEPAGE • DMD: DMD_CODEPAGE	See the following topics in *z/OS Communications Server: IP Configuration Reference*: • Syslog daemon • IKE daemon • Network security services server • Defense Manager daemon
Specify the TCP/IP stack name to be used with TRMD.	Use the **-p** start option in your TRMD cataloged procedure, or on the z/OS UNIX shell command, when starting TRMD. The **-p** start option overrides the resolver configuration file.	• TRMD in *z/OS Communications Server: IP Configuration Guide* • Starting the traffic regulation manager daemon (TRMD) from the z/OS shell in *z/OS Communications Server: IP Configuration Reference*

MVS console support for select TCP/IP commands

z/OS V1R11 Communications Server adds support for using selected z/OS UNIX shell commands from the MVS console, the TSO environment, and from IBM Tivoli® NetView for z/OS. The z/OS UNIX shell commands are supported by a new EZACMD command. The following z/OS UNIX shell commands are supported from the MVS console, TSO, and NetView: **trmdstat**, **ipsec**, **nssctl**, and **pasearch**. In addition, the z/OS UNIX **ping** command is supported from the MVS console and NetView.

Restriction: Only the following z/OS UNIX shell commands are supported by the EZACMD command: **trmdstat**, **ipsec**, **nssctl**, **pasearch**, and **ping**.

Dependency: Use of the EZACMD command from the MVS console depends on the System REXX component being configured and enabled.

Using the MVS console support for select TCP/IP commands

If you want to use the MVS console support for select TCP/IP commands, perform the tasks in Table 68.

Table 68. MVS console support for select TCP/IP commands

Task	Procedure	Reference
Enable the use of EZACMD from the MVS console.	Configure and enable the System REXX component on z/OS.	• System REXX in *z/OS MVS Programming: Authorized Assembler Services Guide* • AXR00 (default System REXX data set concatenation) in *z/OS MVS Initialization and Tuning Reference*
Invoke select z/OS Communications Server UNIX commands from the MVS console, TSO, or NetView environments.	Use the new EZACMD command, specifying the z/OS UNIX command as input.	EZACMD command in *z/OS Communications Server: IP System Administrator's Commands*

IBM Health Checker for z/OS DNS server check

z/OS V1R11 Communications Server provides a new z/OS Health Checker for z/OS migration health check to help determine if you are using the BIND9 DNS server on your system. IBM has previously indicated in statements of direction that support of DNS server functions on z/OS will be removed in a future z/OS release.

Dependency: You must start the IBM Health Checker for z/OS before you can use the IBM Health Checker for z/OS enhancements.

Using the IBM Health Checker for z/OS DNS server check

If you want to use this function, perform the task in Table 69.

Table 69. IBM Health Checker for z/OS DNS server check

Task	Procedure	Reference
Use the IBM Health Checker for z/OS migration check support.	Perform the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Review check output for potential migration actions.	See the following topics in *IBM Health Checker for z/OS: User's Guide*: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

SNA and Enterprise Extender

z/OS V1R11 Communications Server includes enhancements to SNA and Enterprise Extender (EE) in the following areas:

- "Display potential model application name"
- "Include data space VIT with INOP dump"
- "HPR performance enhancements" on page 87
- "APPN topology database update enhancements" on page 90
- "Provide ACF/TAP as part of z/OS Communications Server" on page 91

Display potential model application name

In z/OS V1R11 Communications Server, the DISPLAY MODELS command can identify which application model definition will be used to build a dynamic application definition. You can use the DISPLAY MODELS command to prevent dynamic application definitions from being built incorrectly.

Displaying the potential model application name

If you want to use this function, perform the task in Table 70.

Table 70. Display potential model application name

Task	Procedure	Reference
Discover the model application definition that will be used for building the dynamic definition for an application (APPL1).	Perform the following steps: 1. Issue the DISPLAY NET,MODELS,APPL=APPL1 command. 2. Examine the output (message IST2302I is included if a model was found and message IST2303I is included if no model was found). 3. If IST2304I is also displayed, determine if the existence of another resource using the same name will present a problem.	• DISPLAY MODELS in *z/OS Communications Server: SNA Operation* • Shadow resources in *z/OS Communications Server: SNA Network Implementation Guide*

Include data space VIT with INOP dump

In z/OS V1R11 Communications Server, the VTAM INOP dump processing automatically captures the VTAM internal trace (VIT) data space (ISTITDS1) in the dump when the VIT data space is in use.

VTAM INOP dump processing automatically specifies the inclusion of the data space VIT (ISTITDS1) in all INOP dumps. To make the inclusion of the data space effective in all cases, you might need to increase the size of your system dump data sets to accommodate the possible increase in size of INOP dumps. To use the function, you must use the additional information included in a complete INOP dump. These tasks are described in Table 71.

Table 71. Include data space VIT with INOP dump

Task	Procedure	Reference
Ensure that your system dump data sets are large enough to accommodate the potential increase of 10 to 50 megabytes in the size of INOP dumps.	Perform the following steps: 1. Examine your system dump data set allocation procedure. 2. Increase the size of the data sets by up to 50 megabytes as needed to relieve constraint.	A - allocate new data set in *z/OS ISPF User's Guide Vol II*
Ensure that the data space VIT is active on the system so that additional VIT data will be captured by an INOP dump.	Do one of the following: • Activate the data space VIT when VTAM starts by coding the DSPSIZE operand with a value of 1 through 5 (5 is suggested) on any TRACE,TYPE=VTAM,MODE=INT start option that is included in the VTAM start list or on the VTAM START command. • Activate the VIT data space after VTAM starts by issuing the MODIFY *vtamproc*,TRACE,TYPE=VTAM command; include the DSPSIZE operand with a value of 1 through 5 (5 is suggested).	• TRACE for MODULE, STATE (with OPTION), or VTAM internal trace in *z/OS Communications Server: SNA Resource Definition Reference* • MODIFY TRACE command in *z/OS Communications Server: SNA Operation*
Set up VTAM to take an INOP dump when a link inoperative situation occurs.	Do one of the following: • Activate INOPDUMP when VTAM starts by coding INOPDUMP=ON in the VTAM start list or on the VTAM START command. • Activate INOPDUMP after VTAM starts by issuing the MODIFY *vtamproc*,INOPDUMP=ON command. Optionally, specify a TRLE name.	• INOPDUMP start option in *z/OS Communications Server: SNA Resource Definition Reference* • MODIFY INOPDUMP command in *z/OS Communications Server: SNA Operation*
Diagnose problems using the VIT data in the INOP dump.	Use the VIT entries in ISTITDS1 that provide a longer history of traced events than the VIT in ECSA.	• *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures* • *z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT*

HPR performance enhancements

z/OS V1R11 Communications Server improves high performance routing (HPR) performance in the following ways:

- A new progressive-mode adaptive rate-based (ARB) flow control algorithm increases performance in virtualized or CPU-constrained environments.
- Unproductive path switches are reduced or eliminated when an HPR endpoint is unresponsive.
- ECSA and CSM storage utilization of HPR control blocks is reduced.
- Storage and CPU usage are reduced when packet loss occurs.

Restriction: Progressive-mode ARB applies only to one-hop HPR pipes that traverse Enterprise Extender (EE) connections (which includes a single physical hop across a two-hop EE virtual routing node [VRN]).

Coexistence considerations for HPR performance enhancements

If you are enabling the new ARB level as the HPR flow control algorithm on z/OS V1R11 Communications Server, you must apply the PTFs for APAR OA26490 on prior releases of z/OS Communications Server. The PTFs for APAR OA26490 are required to prevent a prior release from regressing its HPR pipes to base-mode ARB.

Table 72 indicates the PTFs for APAR OA26490 that are required to make the supported releases compatible with V1R11.

Table 72. HPR performance enhancements coexistence PTF APARs

z/OS Communications Server version	PTF for APAR OA26490
V1R8	UA44024
V1R9	UA44025
V1R10	UA44023

For VTAM to successfully negotiate the use of progressive-mode ARB to distributed Communications Servers or to other HPR products, those products must implement the logic needed to support progressive-mode ARB. If the destination HPR platform does not support progressive-mode ARB, the ARB mode is negotiated to either base-mode ARB or responsive-mode ARB.

The progressive-mode ARB enhancement is in the Version 6.4 release of the following products:

- Communications Server for Windows®
- Communications Server for AIX®
- Communications Server for Linux for System z (s390x)
- Communications Server for Linux (i686, x84_64, ppc64)

Using the HPR performance enhancements

If you want to use this function, perform the tasks in Table 73.

Table 73. HPR performance enhancements

Task	Procedure	Reference
Delay the start of HPR path switching logic for 5 seconds for all HPR connections.	Specify HPRPSDLY=5 in the appropriate ATCSTRxx VTAM start list or on the VTAM START command. Optionally, when VTAM is active, issue the MODIFY *procname*,VTAMOPTS, HPRPSDLY=5 command.	• HPRPSDLY start option in *z/OS Communications Server: SNA Resource Definition Reference* • START command and MODIFY VTAMOPTS command in *z/OS Communications Server: SNA Operation*

Table 73. HPR performance enhancements (continued)

Task	Procedure	Reference
Delay the start of HPR path switching logic for 15 seconds for some Enterprise Extender connections.	Specify HPRPSDLY=15 on the following definition statements: • For Enterprise Extender connection networks, define this parameter on the connection network GROUP definition statements in the EE XCA major node. • For dial-in Enterprise Extender connections that have associated PUs that are dynamically created, define this parameter on the model major node (DYNTYPE=EE) PU definition statement. • For predefined Enterprise Extender connections, define this parameter on the PU definition statement in the switched major node.	See the following topics in *z/OS Communications Server: SNA Resource Definition Reference*: • HPRPSDLY XCA major node • HPRPSDLY model major node • HPRPSDLY switched major node
Delay the start of HPR path switching logic long enough to allow the Enterprise Extender Keep-Alive mechanism to make the EE connection inoperable if connectivity to the partner is lost.	Specify HPRPSDLY=EEDELAY on the following definition statements: • For Enterprise Extender connection networks, define this parameter on the connection network GROUP definition statements in the EE XCA major node. • For dial-in Enterprise Extender connections that have their associated PUs dynamically created, define this parameter on the model major node (DYNTYPE=EE) PU definition statement. • For predefined Enterprise Extender connections, define this parameter on the PU definition statement in the switched major node.	See the following topics in *z/OS Communications Server: SNA Resource Definition Reference*: • HPRPSDLY XCA major node • HPRPSDLY model major node • HPRPSDLY switched major node
Display the HPR path switch delay value associated with a specific HPR pipe.	Perform the following steps: 1. Issue the DISPLAY ID=*rtp_pu*,HPRDIAG=YES command. 2. Locate the path switch information in the HPRDIAG output. The value is displayed in message IST2271I.	DISPLAY ID command in *z/OS Communications Server: SNA Operation*

Table 73. HPR performance enhancements (continued)

Task	Procedure	Reference
Designate that progressive-mode ARB is to be used for an EE connection.	Specify the new HPREEARB keyword on the following definition statements: • For Enterprise Extender connection networks, define this parameter on the connection network GROUP definition statements in the EE XCA major node. • For dial-in Enterprise Extender connections that have their associated PUs dynamically created, define this parameter on the model major node (DYNTYPE=EE) PU definition statement. • For predefined Enterprise Extender connections, define this parameter on the PU definition statement in the switched major node.	See the following topics in *z/OS Communications Server: SNA Resource Definition Reference*: • HPREEARB XCA major node • HPREEARB model major node • HPREEARB switched major node
Determine which ARB mode is being used for a specific HPR pipe.	Perform the following steps: 1. Issue the DISPLAY ID=*rtp_pu*,HPRDIAG=YES command. 2. Locate the ARB information in the HPRDIAG output. • If message IST1697I is present, then the responsive-mode ARB algorithm is being used. • If message IST2267I is present, then progressive-mode ARB algorithm is being used. • If neither message IST1697I nor IST2267I is present, then the base-mode ARB algorithm is being used.	DISPLAY ID command in *z/OS Communications Server: SNA Operation*

APPN topology database update enhancements

z/OS V1R11 Communications Server enhances APPN topology database update (TDU) processing in the following ways:

- Topology updates sent to partner network nodes in TDUs will now include unknown topology control vectors based on each partner node's ability to receive them. Any topology control vectors added since the original APPN architecture are considered to be unknown vectors. Unknown topology vectors are not sent to a partner network node that does not have this support. Previously, unknown topology control vectors were not included in TDUs sent to any partner network nodes if at least one partner network node did not support the receipt of unknown vectors.
- Serviceability enhancements aid in the identification of the network nodes involved in a TDU war, which is the endless exchange of TDUs in contention over the same topology resource that results in continuous performance degradation of the APPN network.

Using APPN topology database update enhancements

If you want to use this function, perform the task in Table 74.

Table 74. APPN topology database update enhancements

Task	Procedure	Reference
Determine when TDU diagnostic information is appended with topology control vectors in a TDU if updates are made by this network node to the Resource Sequence Number (RSN) of the node or transmission group (TG).	Specify a TDUDIAG start option value in the appropriate ATCSTRxx VTAM start list or on the VTAM START command: • TDUDIAG=ALWAYS always appends TDU diagnostic information. • TDUDIAG=NEVER never appends TDU diagnostic information. • TDUDIAG=*threshold* appends TDU diagnostic information after this network node has updated the RSN the specified number of times. Optionally, when VTAM is active, issue the MODIFY *procname*,VTAMOPTS, TDUDIAG=*value* command with a TDUDIAG value.	• TDUDIAG start option in *z/OS Communications Server: SNA Resource Definition Reference* • START command and MODIFY VTAMOPTS command in *z/OS Communications Server: SNA Operation*

Provide ACF/TAP as part of z/OS Communications Server

z/OS V1R11 Communications Server includes Advanced Communications Function/Trace Analysis Program (ACF/TAP). ACF/TAP was previously included only as part of the Advanced Communications Function/System Support Program (ACF/SSP) product. ACF/TAP provides a full set of functions to format trace information, including VTAM buffer traces, VTAM internal traces, and NCP traces.

Using ACF/TAP as part of z/OS Communications Server

If you want to use this function, perform the task in Table 75.

Table 75. Provide ACF/TAP as part of z/OS Communications Server

Task	Procedure	Reference
Format VTAM internal traces.	Specify the ACF/TAP INPUT=VIT control parameter.*z/OS Communications Server: ACF/TAP Trace Analysis Handbook*	ACF/TAP parameters in *z/OS Communications Server: ACF/TAP Trace Analysis Handbook*
Format VTAM buffer traces.	Specify the ACF/TAP INPUT=BUFFER control parameter.	ACF/TAP parameters in *z/OS Communications Server: ACF/TAP Trace Analysis Handbook*
Format line traces.	Specify the ACF/TAP INPUT=LINE control parameter.	ACF/TAP parameters in *z/OS Communications Server: ACF/TAP Trace Analysis Handbook*
Format generalized path information unit (PIU) traces.	Specify ACF/TAP INPUT=GPT control parameter.	ACF/TAP parameters in *z/OS Communications Server: ACF/TAP Trace Analysis Handbook*
Format scanner interface traces.	Specify the ACF/TAP INPUT=LINE control parameter.	ACF/TAP parameters in *z/OS Communications Server: ACF/TAP Trace Analysis Handbook*

Table 75. Provide ACF/TAP as part of z/OS Communications Server (continued)

Task	Procedure	Reference
Format network control program (NCP) transmission group traces.	Specify the ACF/TAP INPUT=LINE control parameter.	ACF/TAP parameters in *z/OS Communications Server: ACF/TAP Trace Analysis Handbook*

System management and monitoring

z/OS V1R11 Communications Server includes enhancements to system management and monitoring in the following areas:

- "IBM Health Checker for z/OS RFC 4301 compliance"
- "Network management enhancements"
- "Verbose Ping" on page 96

IBM Health Checker for z/OS RFC 4301 compliance

z/OS V1R11 Communications Server includes a new z/OS Health Checker for z/OS migration health check. This migration health check helps you determine whether IPSec filter rules that are not in compliance with RFC 4301 are active on your current systems. The check also provides guidance on the migration procedures and options available to migrate such IPSec filter rules to become compliant with RFC 4301.

Dependency: IBM Health Checker for z/OS must be active for you to use this function.

Using the IBM Health Checker for z/OS RFC 4301 compliance

If you want to use this function, perform the task in Table 76.

Table 76. IBM Health Checker for z/OS RFC 4301 compliance

Task	Procedure	Reference
Use the migration health check.	Perform the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Review the check output for potential migration actions.	See the following topics in *IBM Health Checker for z/OS: User's Guide*: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

Network management enhancements

z/OS V1R11 Communications Server enhances its network management functions to provide the following information:

- "Stack configuration data"
- "Detailed CSM usage" on page 93
- "OSA network traffic analyzer data" on page 94
- "Sysplex networking data" on page 95

Stack configuration data

z/OS V1R11 Communications Server provides TCP/IP stack profile information in a new SMF 119 event record. The same information is also provided in response to a new GetProfile request for the TCP/IP Callable NMI.

The new SMF 119 event record is subtype 4 and is written to the MVS SMF data sets. The new SMF 119 record can also be obtained from the real-time TCP/IP network monitoring NMI (SYSTCPSM). The new SMF record provides the initial profile information, as well as information about changes to the profile caused by VARY TCPIP,,OBEYFILE processing.

The new GetProfile request for the TCP/IP Callable NMI, EZBNMIFR, provides complete profile information. Network management applications can use a combination of the GetProfile request and the new SMF 119 event records that are created during VARY TCPIP,,OBEYFILE command processing to monitor changes to the TCP/IP profile settings.

Obtaining stack configuration data: If you want to obtain TCP/IP stack configuration data, perform the appropriate tasks in Table 77.

Table 77. NMI stack configuration data

Task	Procedure	Reference
Configure the creation of the SMF 119 subtype 4 event records that provide TCP/IP profile information.	Specify SMFCONFIG TYPE119 PROFILE in the PROFILE.TCPIP configuration file.	SMFCONFIG statement in *z/OS Communications Server: IP Configuration Reference*
Optionally, configure the real-time TCP/IP network monitoring NMI (SYSTCPSM) to support the SMF 119 subtype 4 event records.	Specify NETMONITOR SMFSERVICE PROFILE in the PROFILE.TCPIP configuration file.	NETMONITOR statement in *z/OS Communications Server: IP Configuration Reference*
Enable applications to obtain the SMF 119 subtype 4 event records from the real-time TCP/IP network monitoring NMI (SYSTCPSM).	Configure the user IDs that are associated with the applications to access the SYSTCPSM NMI interface.	Real-time TCP/IP network monitoring NMI: Configuration and enablement in *z/OS Communications Server: IP Programmer's Guide and Reference*
Obtain TCP/IP stack profile information from the TCP/IP Callable NMI.	Develop or enhance an application to use the new TCP/IP Callable NMI request, GetProfile.	TCP/IP callable NMI (EZBNMIFR) in *z/OS Communications Server: IP Programmer's Guide and Reference*

Detailed CSM usage

The SNA network management interface (NMI) in z/OS V1R11 Communications Server provides additional storage ownership statistics in response to the Communication Storage Manager (CSM) statistics request. You can request all ownership statistics or a subset of statistics that is based on ASID values.

Restriction: The monitor application must explicitly request the additional storage ownership statistics on the CSM statistics request.

Obtaining detailed CSM usage: If you want to obtain detailed CSM usage data, perform the appropriate tasks in Table 78 on page 94.

Table 78. Network management interface enhancements - detailed CSM usage

Task	Procedure	Reference
Update your SNA network monitoring NMI to collect all CSM storage ownership statistics.	Perform the following steps: 1. Examine the initialization record returned by the VTAM server to verify that VTAM supports the inclusion of request filters on the CSM statistics request. 2. Build a CSM statistics request. Include a request filter record that specifies a 0 as the ASID value. 3. Send a CSM statistics request to the VTAM server. 4. Read the CSM statistics response and parse the new CSM storage owner output section record to obtain the new storage ownership statistics.	SNA network monitoring NMI in *z/OS Communications Server: IP Programmer's Guide and Reference*
Update your SNA network monitoring NMI to collect CSM storage ownership statistics for a specific ASID.	Perform the following steps: 1. Examine the initialization record returned by the VTAM server to verify that VTAM supports the inclusion of request filters on the CSM statistics request. 2. Build a CSM statistics request. Include up to four request filter records, where each individual record specifies a single ASID value for which storage ownership statistics are requested. 3. Send a CSM statistics request to the VTAM server. 4. Read the CSM statistics response and parse the new CSM storage owner output section record to obtain the new storage ownership statistics.	SNA network monitoring NMI in *z/OS Communications Server: IP Programmer's Guide and Reference*

OSA network traffic analyzer data

In z/OS V1R11 Communications Server, the OSA-Express network traffic analyzer trace facility provides real time trace collection similar to the SYSTCPDA packet trace collection.

Dependencies:

- To enable the OSA-Express network traffic analyzer, you must be running at least an IBM System z9 EC or z9 BC and OSA-Express2 feature in QDIO mode. See the 2094DEVICE Preventive Service Planning (PSP) and the 2096DEVICE Preventive Service Planning (PSP) buckets for more information.
- To use this function, you must configure an AF_UNIX NETWORK statement in the BPXPRMxx parmlib member.

Obtaining OSA network traffic analyzer data: If you want to obtain OSA network traffic analyzer data, perform the appropriate tasks in Table 79 on page 95.

Table 79. OSA network traffic analyzer data

Task	Procedure	Reference

Define the AF_UNIX socket domain (necessary only if AF_UNIX socket is not already defined).	Add the following to the BPXPRMxx parmlib member:
	`FILESYSTYPE TYPE(UDS)`
	`ENTRYPOINT (BPXTUINT)`
	`NETWORK DOMAINNAME(AF_UNIX)`
	`DOMAINNUMBER(1) MAXSOCKETS(`*nnn*`)`
	`TYPE(UDS)`
	
	where *nnn* is the maximum number of AF_UNIX sockets.
		z/OS UNIX System Services Planning

Enable the OSAENTA services on this TCPIP stack.	Specify the NTATRCSERVICE parameter on the NETMONITOR profile statement.	NETMONITOR in *z/OS Communications Server: IP Configuration Reference*

Optionally, limit access to these trace services to specific applications by using RACF (or an equivalent external security manager).	If you are using RACF, issue the following commands:
	`SETROPTS CLASSACT(SERVAUTH)`
	`RDEFINE SERVAUTH`
	`EZB.NETMGMT.`*`sysname.tcpprocname`*`.*`
	`UACC(NONE)`
	`PERMIT EZB.NETMGMT.`*`sysname.tcpprocname`*`.*`
	`USERID(`*`userid`*`)`
	`SETROPTS RACLIST(REFRESH)`
	
	where *userid* is the client's user ID that is permitted.
	
	This generic profile covers all the TCP/IP Network Management interfaces. Create individual profiles to attain granularity.
		• *z/OS Communications Server: IP Configuration Guide*
		• *z/OS Communications Server: IP Configuration Reference*

Update or create an application that uses the real-time asynchronous data collection and formatting interfaces.	Review the instructions in *z/OS Communications Server: IP Programmer's Guide and Reference*.	Real-time TCP/IP network monitoring NMI in *z/OS Communications Server: IP Programmer's Guide and Reference*

Sysplex networking data

In z/OS V1R11 Communications Server, the TCP/IP Callable NMI, EZBNMIFR provides sysplex networking data. The new request types are as follows:

- GetSysplexXCF - Obtains information about dynamic XCF addresses for all TCP/IP stacks in the sysplex
- GetDVIPAList - Obtains information about dynamic virtual IP addresses (DVIPAs)
- GetDVIPAPortDist - Obtains information about DVIPA port distribution
- GetDVIPARoute - Obtains information about DVIPA routes
- GetDVIPAConnRTab - Obtains information about DVIPA connections

The DVIPA information provided by EZBNMIFR is similar to information that can be obtained from the IBM TCP/IP MVS Enterprise-specific MIB using SNMP.

Obtaining sysplex networking data: If you want to obtain sysplex networking data, perform the task in Table 80 on page 96.

Table 80. NMI sysplex networking data

Task	Procedure	Reference
Update your NMI application that uses the EZBNMIFR interface to collect the sysplex networking data.	Specify one of the new request types when invoking the EZBNMIFR interface: • Use request type NWMSYXCFTYPE to obtain information about dynamic XCF addresses for all TCP/IP stacks in the sysplex. • Use request type NWMDVLISTTYPE to obtain information about DVIPAs. • Use request type NWMDVPORTDISTTYPE to obtain information about DVIPA port distribution. • Use request type NWMDVROUTETYPE to obtain information about DVIPA routes. • Use request type NWMDVCONNRTABTYPE to obtain information about DVIPA connections.	TCP/IP callable NMI (EZBNMIFR) in *z/OS Communications Server: IP Programmer's Guide and Reference*

Verbose Ping

In z/OS V1R11 Communications Server, the Verbose/-v parameter causes the Ping command to display details of the echo reply packets that have been received, and summary statistics regarding the echo packets (number of requests sent, number of replies received, and number of packets lost), and the round-trip times (minimum, maximum, average, and standard deviation) based on the response times from the echo replies that were received.

Using the Verbose Ping command

If you want to use this function, perform the task in Table 81.

Table 81. Verbose Ping

Task	Procedure	Reference
Use the Ping command to display details for the echo reply packets that were received and to display summary statistics.	Invoke the TSO PING command with the Verbose parameter, or the z/OS UNIX **ping** or **oping** command with the -v parameter, and vary the size of the outbound echo request packet.	Ping in *z/OS Communications Server: IP System Administrator's Commands*

Virtualization

z/OS V1R11 Communications Server includes enhancements to virtualization in the following areas:

- "QDIO enhancements for Workload Manager IO priority"
- "QDIO support for OSA interface isolation" on page 97

QDIO enhancements for Workload Manager IO priority

z/OS V1R11 Communications Server introduces a new WLMPRIORITYQ parameter on the GLOBALCONFIG profile statement. You can use this parameter to establish a mapping of Workload Manager (WLM) service classes to outbound Queued Direct I/O (QDIO) priorities. This mapping is used to determine the

QDIO write priority for outbound packets. This function automatically extends the preferential treatment of the most important workloads for a business through the QDIO device driver all the way to the LAN.

You can also use the WLMPRIORITYQ parameter to apply the outbound priority to forwarded packets.

Restrictions:

- Prioritization using the WLM service class is effective only when enabled and when the ToS or Traffic Class value is 0.
- Prioritization using the WLM service class is ineffective for interfaces other than OSA-Express features in QDIO mode.
- Prioritization of forwarded packets is ineffective unless DATAGRAMFWD is specified on the IPCONFIG statement, the IPCONFIG6 statement, or both statements.
- The WLMPRIORITYQ setting for forwarded packets has no effect on accelerated packets.

Using the QDIO enhancements for WLM IO priority

If you want to use this function, perform the tasks in Table 82.

Table 82. QDIO enhancements for WLM IO priority

Task	Procedure	Reference
Enable the WLMPRIORITYQ parameter using the default mapping.	Perform the following steps: 1. Specify the WLMPRIORITYQ parameter on the GLOBALCONFIG statement in the TCP/IP profile. 2. Start TCP/IP or issue the VARY OBEYFILE command.	GLOBALCONFIG in *z/OS Communications Server: IP Configuration Reference*
Enable the WLMPRIORITYQ parameter using a mapping other than the default.	Perform the following steps: 1. Specify the WLMPRIORITYQ IOPRIn *control_values* parameter on the GLOBALCONFIG statement in the TCP/IP profile. 2. Start TCP/IP or issue the VARY OBEYFILE command.	GLOBALCONFIG in *z/OS Communications Server: IP Configuration Reference*
Display the current WLMPRIORITYQ mapping.	Issue the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*

QDIO support for OSA interface isolation

z/OS V1R11 Communications Server enables a stack that is using an OSA-Express feature to prevent packets from flowing directly between two stacks that are sharing the OSA device. This is called connection isolation and when it is in effect, the OSA-Express feature discards packets whose next-hop address was registered by a sharing stack. The OSA-Express feature requires that both stacks that share the port be non-isolated for direct routing to occur.

Restrictions:

- OSA-Express connection isolation is supported only for OSA-Express features in QDIO mode.

- OSA-Express connection isolation is not supported when the OSA-Express feature is defined using a DEVICE and LINK statement.

Dependency: This function is limited to OSA-Express2 or OSA-Express3 Ethernet features in QDIO mode and running at least an IBM System z9 Enterprise Class (EC) or z9 Business Class (BC). See the 2094DEVICE, 2096DEVICE, 2097DEVICE, or 2098DEVICE Preventive Service Planning (PSP) bucket for more information.

Using the QDIO support for OSA interface isolation

If you want to use this function, perform the appropriate tasks in Table 83.

Table 83. QDIO support for OSA interface isolation

Task	Procedure	Reference
Determine the Licensed Internal Code level of the OSA-Express feature.	Use the VTAM DISPLAY TRL command to determine the OSA-Express Licensed Internal Code level that is currently installed. See the DISPLAY TRL command for more information.	DISPLAY TRL command in *z/OS Communications Server: SNA Operation*
Enable OSA-Express connection isolation.	Perform the following steps: 1. Specify the ISOLATE parameter on the INTERFACE statements in the TCP/IP profile. 2. Start TCP/IP.	INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces in *z/OS Communications Server: IP Configuration Reference*
Display information about the OSA-Express connection isolation.	Issue the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d report in *z/OS Communications Server: IP System Administrator's Commands*

Appendix A. Related protocol specifications

This appendix lists the related protocol specifications (RFCs) for TCP/IP. The Internet Protocol suite is still evolving through requests for comments (RFC). New protocols are being designed and implemented by researchers and are brought to the attention of the Internet community in the form of RFCs. Some of these protocols are so useful that they become recommended protocols. That is, all future implementations for TCP/IP are recommended to implement these particular functions or protocols. These become the *de facto* standards, on which the TCP/IP protocol suite is built.

You can request RFCs through electronic mail, from the automated Network Information Center (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` or at:

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

Hard copies of all RFCs are available from the NIC, either individually or by subscription. Online copies are available at the following Web address: http://www.rfc-editor.org/rfc.html.

See "Internet drafts" on page 115 for draft RFCs implemented in this and previous Communications Server releases.

Many features of TCP/IP Services are based on the following RFCs:

RFC	Title and Author
RFC 652	*Telnet output carriage-return disposition option* D. Crocker
RFC 653	*Telnet output horizontal tabstops option* D. Crocker
RFC 654	*Telnet output horizontal tab disposition option* D. Crocker
RFC 655	*Telnet output formfeed disposition option* D. Crocker
RFC 657	*Telnet output vertical tab disposition option* D. Crocker
RFC 658	*Telnet output linefeed disposition* D. Crocker
RFC 698	*Telnet extended ASCII option* T. Mock
RFC 726	*Remote Controlled Transmission and Echoing Telnet option* J. Postel, D. Crocker
RFC 727	*Telnet logout option* M.R. Crispin
RFC 732	*Telnet Data Entry Terminal option* J.D. Day
RFC 733	*Standard for the format of ARPA network text messages* D. Crocker, J. Vittal, K.T. Pogran, D.A. Henderson

RFC 734 *SUPDUP Protocol* M.R. Crispin

RFC 735 *Revised Telnet byte macro option* D. Crocker, R.H. Gumpertz

RFC 736 *Telnet SUPDUP option* M.R. Crispin

RFC 749 *Telnet SUPDUP—Output option* B. Greenberg

RFC 765 *File Transfer Protocol specification* J. Postel

RFC 768 *User Datagram Protocol* J. Postel

RFC 779 *Telnet send-location option* E. Killian

RFC 783 *TFTP Protocol (revision 2)* K.R. Sollins

RFC 791 *Internet Protocol* J. Postel

RFC 792 *Internet Control Message Protocol* J. Postel

RFC 793 *Transmission Control Protocol* J. Postel

RFC 820 *Assigned numbers* J. Postel

RFC 821 *Simple Mail Transfer Protocol* J. Postel

RFC 822 *Standard for the format of ARPA Internet text messages* D. Crocker

RFC 823 *DARPA Internet gateway* R. Hinden, A. Sheltzer

RFC 826 *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware* D. Plummer

RFC 854 *Telnet Protocol Specification* J. Postel, J. Reynolds

RFC 855 *Telnet Option Specification* J. Postel, J. Reynolds

RFC 856 *Telnet Binary Transmission* J. Postel, J. Reynolds

RFC 857 *Telnet Echo Option* J. Postel, J. Reynolds

RFC 858 *Telnet Suppress Go Ahead Option* J. Postel, J. Reynolds

RFC 859 *Telnet Status Option* J. Postel, J. Reynolds

RFC 860 *Telnet Timing Mark Option* J. Postel, J. Reynolds

RFC 861 *Telnet Extended Options: List Option* J. Postel, J. Reynolds

RFC 862 *Echo Protocol* J. Postel

RFC 863 *Discard Protocol* J. Postel

RFC 864 *Character Generator Protocol* J. Postel

RFC 865 *Quote of the Day Protocol* J. Postel

RFC 868 *Time Protocol* J. Postel, K. Harrenstien

RFC 877 *Standard for the transmission of IP datagrams over public data networks* J.T. Korb

RFC 883 *Domain names: Implementation specification* P.V. Mockapetris

RFC 884 *Telnet terminal type option* M. Solomon, E. Wimmers

RFC 885 *Telnet end of record option* J. Postel

RFC 894 *Standard for the transmission of IP datagrams over Ethernet networks* C. Hornig

RFC 896 *Congestion control in IP/TCP internetworks* J. Nagle

RFC 903 *Reverse Address Resolution Protocol* R. Finlayson, T. Mann, J. Mogul, M. Theimer

RFC 904 *Exterior Gateway Protocol formal specification* D. Mills

RFC 919 *Broadcasting Internet Datagrams* J. Mogul

RFC 922 *Broadcasting Internet datagrams in the presence of subnets* J. Mogul

RFC 927 *TACACS user identification Telnet option* B.A. Anderson

RFC 933 *Output marking Telnet option* S. Silverman

RFC 946 *Telnet terminal location number option* R. Nedved

RFC 950 *Internet Standard Subnetting Procedure* J. Mogul, J. Postel

RFC 952 *DoD Internet host table specification* K. Harrenstien, M. Stahl, E. Feinler

RFC 959 *File Transfer Protocol* J. Postel, J.K. Reynolds

RFC 961 *Official ARPA-Internet protocols* J.K. Reynolds, J. Postel

RFC 974 *Mail routing and the domain system* C. Partridge

RFC 1001 *Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and methods* NetBios Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, End-to-End Services Task Force

RFC 1002 *Protocol Standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications* NetBios Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, End-to-End Services Task Force

RFC 1006 *ISO transport services on top of the TCP: Version 3* M.T. Rose, D.E. Cass

RFC 1009 *Requirements for Internet gateways* R. Braden, J. Postel

RFC 1011 *Official Internet protocols* J. Reynolds, J. Postel

RFC 1013 *X Window System Protocol, version 11: Alpha update April 1987* R. Scheifler

RFC 1014 *XDR: External Data Representation standard* Sun Microsystems

RFC 1027 *Using ARP to implement transparent subnet gateways* S. Carl-Mitchell, J. Quarterman

RFC 1032 *Domain administrators guide* M. Stahl

RFC 1033 *Domain administrators operations guide* M. Lottor

RFC 1034 *Domain names—concepts and facilities* P.V. Mockapetris

RFC 1035 *Domain names—implementation and specification* P.V. Mockapetris

RFC 1038 *Draft revised IP security option* M. St. Johns

RFC 1041 *Telnet 3270 regime option* Y. Rekhter

RFC 1042 *Standard for the transmission of IP datagrams over IEEE 802 networks* J. Postel, J. Reynolds

RFC 1043 *Telnet Data Entry Terminal option: DODIIS implementation* A. Yasuda, T. Thompson

RFC 1044 *Internet Protocol on Network System's HYPERchannel: Protocol specification* K. Hardwick, J. Lekashman

RFC 1053 *Telnet X.3 PAD option* S. Levy, T. Jacobson

RFC 1055 *Nonstandard for transmission of IP datagrams over serial lines: SLIP* J. Romkey

RFC 1057 *RPC: Remote Procedure Call Protocol Specification: Version 2* Sun Microsystems

RFC 1058 *Routing Information Protocol* C. Hedrick

RFC 1060 *Assigned numbers* J. Reynolds, J. Postel

RFC 1067 *Simple Network Management Protocol* J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin

RFC 1071 *Computing the Internet checksum* R.T. Braden, D.A. Borman, C. Partridge

RFC 1072 *TCP extensions for long-delay paths* V. Jacobson, R.T. Braden

RFC 1073 *Telnet window size option* D. Waitzman

RFC 1079 *Telnet terminal speed option* C. Hedrick

RFC 1085 *ISO presentation services on top of TCP/IP based internets* M.T. Rose

RFC 1091 *Telnet terminal-type option* J. VanBokkelen

RFC 1094 *NFS: Network File System Protocol specification* Sun Microsystems

RFC 1096 *Telnet X display location option* G. Marcy

RFC 1101 *DNS encoding of network names and other types* P. Mockapetris

RFC 1112 *Host extensions for IP multicasting* S.E. Deering

RFC 1113 *Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures* J. Linn

RFC 1118 *Hitchhikers Guide to the Internet* E. Krol

RFC 1122 *Requirements for Internet Hosts—Communication Layers* R. Braden, Ed.

RFC 1123 *Requirements for Internet Hosts—Application and Support* R. Braden, Ed.

RFC 1146 *TCP alternate checksum options* J. Zweig, C. Partridge

RFC 1155 *Structure and identification of management information for TCP/IP-based internets* M. Rose, K. McCloghrie

RFC 1156 *Management Information Base for network management of TCP/IP-based internets* K. McCloghrie, M. Rose

RFC 1157 *Simple Network Management Protocol (SNMP)* J. Case, M. Fedor, M. Schoffstall, J. Davin

RFC 1158 *Management Information Base for network management of TCP/IP-based internets: MIB-II* M. Rose

RFC 1166 *Internet numbers* S. Kirkpatrick, M.K. Stahl, M. Recker

RFC 1179 *Line printer daemon protocol* L. McLaughlin

RFC 1180 *TCP/IP tutorial* T. Socolofsky, C. Kale

RFC 1183 *New DNS RR Definitions* C.F. Everhart, L.A. Mamakos, R. Ullmann, P.V. Mockapetris

RFC 1184 *Telnet Linemode Option* D. Borman

RFC 1186 *MD4 Message Digest Algorithm* R.L. Rivest

RFC 1187 *Bulk Table Retrieval with the SNMP* M. Rose, K. McCloghrie, J. Davin

RFC 1188 *Proposed Standard for the Transmission of IP Datagrams over FDDI Networks* D. Katz

RFC 1190 *Experimental Internet Stream Protocol: Version 2 (ST-II)* C. Topolcic

RFC 1191 *Path MTU discovery* J. Mogul, S. Deering

RFC 1198 *FYI on the X window system* R. Scheifler

RFC 1207 *FYI on Questions and Answers: Answers to commonly asked "experienced Internet user" questions* G. Malkin, A. Marine, J. Reynolds

RFC 1208 *Glossary of networking terms* O. Jacobsen, D. Lynch

RFC 1213 *Management Information Base for Network Management of TCP/IP-based internets: MIB-II* K. McCloghrie, M.T. Rose

RFC 1215 *Convention for defining traps for use with the SNMP* M. Rose

RFC 1227 *SNMP MUX protocol and MIB* M.T. Rose

RFC 1228 *SNMP-DPI: Simple Network Management Protocol Distributed Program Interface* G. Carpenter, B. Wijnen

RFC 1229 *Extensions to the generic-interface MIB* K. McCloghrie

RFC 1230 *IEEE 802.4 Token Bus MIB* K. McCloghrie, R. Fox

RFC 1231 *IEEE 802.5 Token Ring MIB* K. McCloghrie, R. Fox, E. Decker

RFC 1236 *IP to X.121 address mapping for DDN* L. Morales, P. Hasse

RFC 1256 *ICMP Router Discovery Messages* S. Deering, Ed.

RFC 1267 *Border Gateway Protocol 3 (BGP-3)* K. Lougheed, Y. Rekhter

RFC 1268 *Application of the Border Gateway Protocol in the Internet* Y. Rekhter, P. Gross

RFC 1269 *Definitions of Managed Objects for the Border Gateway Protocol: Version 3* S. Willis, J. Burruss

RFC 1270 *SNMP Communications Services* F. Kastenholz, ed.

RFC 1285 *FDDI Management Information Base* J. Case

RFC 1315 *Management Information Base for Frame Relay DTEs* C. Brown, F. Baker, C. Carvalho

RFC 1321 *The MD5 Message-Digest Algorithm* R. Rivest

RFC 1323 *TCP Extensions for High Performance* V. Jacobson, R. Braden, D. Borman

RFC 1325 *FYI on Questions and Answers: Answers to Commonly Asked "New Internet User" Questions* G. Malkin, A. Marine

RFC 1327 *Mapping between X.400 (1988)/ISO 10021 and RFC 822* S. Hardcastle-Kille

RFC 1340 *Assigned Numbers* J. Reynolds, J. Postel

RFC 1344 *Implications of MIME for Internet Mail Gateways* N. Bornstein

RFC 1349 *Type of Service in the Internet Protocol Suite* P. Almquist

RFC 1350 *The TFTP Protocol (Revision 2)* K.R. Sollins

RFC 1351 *SNMP Administrative Model* J. Davin, J. Galvin, K. McCloghrie

RFC 1352 *SNMP Security Protocols* J. Galvin, K. McCloghrie, J. Davin

RFC 1353 *Definitions of Managed Objects for Administration of SNMP Parties* K. McCloghrie, J. Davin, J. Galvin

RFC 1354 *IP Forwarding Table MIB* F. Baker

RFC 1356 *Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode* A. Malis, D. Robinson, R. Ullmann

RFC 1358 *Charter of the Internet Architecture Board (IAB)* L. Chapin

RFC 1363 *A Proposed Flow Specification* C. Partridge

RFC 1368 *Definition of Managed Objects for IEEE 802.3 Repeater Devices* D. McMaster, K. McCloghrie

RFC 1372 *Telnet Remote Flow Control Option* C. L. Hedrick, D. Borman

RFC 1374 *IP and ARP on HIPPI* J. Renwick, A. Nicholson

RFC 1381 *SNMP MIB Extension for X.25 LAPB* D. Throop, F. Baker

RFC 1382 *SNMP MIB Extension for the X.25 Packet Layer* D. Throop

RFC 1387 *RIP Version 2 Protocol Analysis* G. Malkin

RFC 1388 *RIP Version 2 Carrying Additional Information* G. Malkin

RFC 1389 *RIP Version 2 MIB Extensions* G. Malkin, F. Baker

RFC 1390 *Transmission of IP and ARP over FDDI Networks* D. Katz

RFC 1393 *Traceroute Using an IP Option* G. Malkin

RFC 1398 *Definitions of Managed Objects for the Ethernet-Like Interface Types* F. Kastenholz

RFC 1408 *Telnet Environment Option* D. Borman, Ed.

RFC 1413 *Identification Protocol* M. St. Johns

RFC 1416 *Telnet Authentication Option* D. Borman, ed.

RFC 1420 *SNMP over IPX* S. Bostock

RFC 1428 *Transition of Internet Mail from Just-Send-8 to 8bit-SMTP/MIME* G. Vaudreuil

RFC 1442 *Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1443 *Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1445 *Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Galvin, K. McCloghrie

RFC 1447 *Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)* K. McCloghrie, J. Galvin

RFC 1448 *Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1464 *Using the Domain Name System to Store Arbitrary String Attributes* R. Rosenbaum

RFC 1469 *IP Multicast over Token-Ring Local Area Networks* T. Pusateri

RFC 1483 *Multiprotocol Encapsulation over ATM Adaptation Layer 5* Juha Heinanen

RFC 1514 *Host Resources MIB* P. Grillo, S. Waldbusser

RFC 1516 *Definitions of Managed Objects for IEEE 802.3 Repeater Devices* D. McMaster, K. McCloghrie

RFC 1521 *MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies* N. Borenstein, N. Freed

RFC 1535 *A Security Problem and Proposed Correction With Widely Deployed DNS Software* E. Gavron

RFC 1536 *Common DNS Implementation Errors and Suggested Fixes* A. Kumar, J. Postel, C. Neuman, P. Danzig, S. Miller

RFC 1537 *Common DNS Data File Configuration Errors* P. Beertema

RFC 1540 *Internet Official Protocol Standards* J. Postel

RFC 1571 *Telnet Environment Option Interoperability Issues* D. Borman

RFC 1572 *Telnet Environment Option* S. Alexander

RFC 1573 *Evolution of the Interfaces Group of MIB-II* K. McCloghrie, F. Kastenholz

RFC 1577 *Classical IP and ARP over ATM* M. Laubach

RFC 1583 *OSPF Version 2* J. Moy

RFC 1591 *Domain Name System Structure and Delegation* J. Postel

RFC 1592 *Simple Network Management Protocol Distributed Protocol Interface Version 2.0* B. Wijnen, G. Carpenter, K. Curran, A. Sehgal, G. Waters

RFC 1594 *FYI on Questions and Answers— Answers to Commonly Asked "New Internet User" Questions* A. Marine, J. Reynolds, G. Malkin

RFC 1644 *T/TCP — TCP Extensions for Transactions Functional Specification* R. Braden

RFC 1646 *TN3270 Extensions for LUname and Printer Selection* C. Graves, T. Butts, M. Angel

RFC 1647 *TN3270 Enhancements* B. Kelly

RFC 1652 *SMTP Service Extension for 8bit-MIMEtransport* J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker

RFC 1664 *Using the Internet DNS to Distribute RFC1327 Mail Address Mapping Tables* C. Allochio, A. Bonito, B. Cole, S. Giordano, R. Hagens

RFC 1693 *An Extension to TCP: Partial Order Service* T. Connolly, P. Amer, P. Conrad

RFC 1695 *Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2* M. Ahmed, K. Tesink

RFC 1701 *Generic Routing Encapsulation (GRE)* S. Hanks, T. Li, D. Farinacci, P. Traina

RFC 1702 *Generic Routing Encapsulation over IPv4 networks* S. Hanks, T. Li, D. Farinacci, P. Traina

RFC 1706 *DNS NSAP Resource Records* B. Manning, R. Colella

RFC 1712 *DNS Encoding of Geographical Location* C. Farrell, M. Schulze, S. Pleitner D. Baldoni

RFC 1713 *Tools for DNS debugging* A. Romao

RFC 1723 *RIP Version 2—Carrying Additional Information* G. Malkin

RFC 1752 *The Recommendation for the IP Next Generation Protocol* S. Bradner, A. Mankin

RFC 1766 *Tags for the Identification of Languages* H. Alvestrand

RFC 1771 *A Border Gateway Protocol 4 (BGP-4)* Y. Rekhter, T. Li

RFC 1794 *DNS Support for Load Balancing* T. Brisco

RFC 1819 *Internet Stream Protocol Version 2 (ST2) Protocol Specification—Version ST2+* L. Delgrossi, L. Berger Eds.

RFC 1826 *IP Authentication Header* R. Atkinson

RFC 1828 *IP Authentication using Keyed MD5* P. Metzger, W. Simpson

RFC 1829 *The ESP DES-CBC Transform* P. Karn, P. Metzger, W. Simpson

RFC 1830 *SMTP Service Extensions for Transmission of Large and Binary MIME Messages* G. Vaudreuil

RFC 1831 *RPC: Remote Procedure Call Protocol Specification Version 2* R. Srinivasan

RFC 1832 *XDR: External Data Representation Standard* R. Srinivasan

RFC 1833 *Binding Protocols for ONC RPC Version 2* R. Srinivasan

RFC 1850 *OSPF Version 2 Management Information Base* F. Baker, R. Coltun

RFC 1854 *SMTP Service Extension for Command Pipelining* N. Freed

RFC 1869 *SMTP Service Extensions* J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker

RFC 1870 *SMTP Service Extension for Message Size Declaration* J. Klensin, N. Freed, K. Moore

RFC 1876 *A Means for Expressing Location Information in the Domain Name System* C. Davis, P. Vixie, T. Goodwin, I. Dickinson

RFC 1883 *Internet Protocol, Version 6 (IPv6) Specification* S. Deering, R. Hinden

RFC 1884 *IP Version 6 Addressing Architecture* R. Hinden, S. Deering, Eds.

RFC 1886 *DNS Extensions to support IP version 6* S. Thomson, C. Huitema

RFC 1888 *OSI NSAPs and IPv6* J. Bound, B. Carpenter, D. Harrington, J. Houldsworth, A. Lloyd

RFC 1891 *SMTP Service Extension for Delivery Status Notifications* K. Moore

RFC 1892 *The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages* G. Vaudreuil

RFC 1894 *An Extensible Message Format for Delivery Status Notifications*K. Moore, G. Vaudreuil

RFC 1901 *Introduction to Community-based SNMPv2* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1902 *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1903 *Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1904 *Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1905 *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1906 *Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1907 *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1908 *Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1912 *Common DNS Operational and Configuration Errors* D. Barr

RFC 1918 *Address Allocation for Private Internets* Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear

RFC 1928 *SOCKS Protocol Version 5* M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones

RFC 1930 *Guidelines for creation, selection, and registration of an Autonomous System (AS)* J. Hawkinson, T. Bates

RFC 1939 *Post Office Protocol-Version 3* J. Myers, M. Rose

RFC 1981 *Path MTU Discovery for IP version 6* J. McCann, S. Deering, J. Mogul

RFC 1982 *Serial Number Arithmetic* R. Elz, R. Bush

RFC 1985 *SMTP Service Extension for Remote Message Queue Starting* J. De Winter

RFC 1995 *Incremental Zone Transfer in DNS* M. Ohta

RFC 1996 *A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)* P. Vixie

RFC 2010 *Operational Criteria for Root Name Servers* B. Manning, P. Vixie

RFC 2011 *SNMPv2 Management Information Base for the Internet Protocol using SMIv2* K. McCloghrie, Ed.

RFC 2012 *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2* K. McCloghrie, Ed.

RFC 2013 *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2* K. McCloghrie, Ed.

RFC 2018 *TCP Selective Acknowledgement Options* M. Mathis, J. Mahdavi, S. Floyd, A. Romanow

RFC 2026 *The Internet Standards Process — Revision 3* S. Bradner

RFC 2030 *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI* D. Mills

RFC 2033 *Local Mail Transfer Protocol* J. Myers

RFC 2034 *SMTP Service Extension for Returning Enhanced Error Codes*N. Freed

RFC 2040 *The RC5, RC5–CBC, RC-5–CBC-Pad, and RC5–CTS Algorithms*R. Baldwin, R. Rivest

RFC 2045 *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies* N. Freed, N. Borenstein

RFC 2052 *A DNS RR for specifying the location of services (DNS SRV)* A. Gulbrandsen, P. Vixie

RFC 2065 *Domain Name System Security Extensions* D. Eastlake 3rd, C. Kaufman

RFC 2066 *TELNET CHARSET Option* R. Gellens

RFC 2080 *RIPng for IPv6* G. Malkin, R. Minnear

RFC 2096 *IP Forwarding Table MIB* F. Baker

RFC 2104 *HMAC: Keyed-Hashing for Message Authentication* H. Krawczyk, M. Bellare, R. Canetti

RFC 2119 *Keywords for use in RFCs to Indicate Requirement Levels* S. Bradner

RFC 2133 *Basic Socket Interface Extensions for IPv6* R. Gilligan, S. Thomson, J. Bound, W. Stevens

RFC 2136 *Dynamic Updates in the Domain Name System (DNS UPDATE)* P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound

RFC 2137 *Secure Domain Name System Dynamic Update* D. Eastlake 3rd

RFC 2163 *Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)* C. Allocchio

RFC 2168 *Resolution of Uniform Resource Identifiers using the Domain Name System* R. Daniel, M. Mealling

RFC 2178 *OSPF Version 2* J. Moy

RFC 2181 *Clarifications to the DNS Specification* R. Elz, R. Bush

RFC 2205 *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification* R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin

RFC 2210 *The Use of RSVP with IETF Integrated Services* J. Wroclawski

RFC 2211 *Specification of the Controlled-Load Network Element Service* J. Wroclawski

RFC 2212 *Specification of Guaranteed Quality of Service* S. Shenker, C. Partridge, R. Guerin

RFC 2215 *General Characterization Parameters for Integrated Service Network Elements* S. Shenker, J. Wroclawski

RFC 2217 *Telnet Com Port Control Option* G. Clarke

RFC 2219 *Use of DNS Aliases for Network Services* M. Hamilton, R. Wright

RFC 2228 *FTP Security Extensions* M. Horowitz, S. Lunt

RFC 2230 *Key Exchange Delegation Record for the DNS* R. Atkinson

RFC 2233 *The Interfaces Group MIB using SMIv2* K. McCloghrie, F. Kastenholz

RFC 2240 *A Legal Basis for Domain Name Allocation* O. Vaughn

RFC 2246 *The TLS Protocol Version 1.0* T. Dierks, C. Allen

RFC 2251 *Lightweight Directory Access Protocol (v3)* M. Wahl, T. Howes, S. Kille

RFC 2253 *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names* M. Wahl, S. Kille, T. Howes

RFC 2254 *The String Representation of LDAP Search Filters* T. Howes

RFC 2261 *An Architecture for Describing SNMP Management Frameworks* D. Harrington, R. Presuhn, B. Wijnen

RFC 2262 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 2271 *An Architecture for Describing SNMP Management Frameworks* D. Harrington, R. Presuhn, B. Wijnen

RFC 2273 *SNMPv3 Applications* D. Levi, P. Meyer, B. Stewartz

RFC 2274 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* U. Blumenthal, B. Wijnen

RFC 2275 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* B. Wijnen, R. Presuhn, K. McCloghrie

RFC 2279 *UTF-8, a transformation format of ISO 10646* F. Yergeau

RFC 2292 *Advanced Sockets API for IPv6* W. Stevens, M. Thomas

RFC 2308 *Negative Caching of DNS Queries (DNS NCACHE)* M. Andrews

RFC 2317 *Classless IN-ADDR.ARPA delegation* H. Eidnes, G. de Groot, P. Vixie

RFC 2320 *Definitions of Managed Objects for Classical IP and ARP Over ATM Using SMIv2 (IPOA-MIB)* M. Greene, J. Luciani, K. White, T. Kuo

RFC 2328 *OSPF Version 2* J. Moy

RFC 2345 *Domain Names and Company Name Retrieval* J. Klensin, T. Wolf, G. Oglesby

RFC 2352 *A Convention for Using Legal Names as Domain Names* O. Vaughn

RFC 2355 *TN3270 Enhancements* B. Kelly

RFC 2358 *Definitions of Managed Objects for the Ethernet-like Interface Types* J. Flick, J. Johnson

RFC 2373 *IP Version 6 Addressing Architecture* R. Hinden, S. Deering

RFC 2374 *An IPv6 Aggregatable Global Unicast Address Format* R. Hinden, M. O'Dell, S. Deering

RFC 2375 *IPv6 Multicast Address Assignments* R. Hinden, S. Deering

RFC 2385 *Protection of BGP Sessions via the TCP MD5 Signature Option*A. Hefferman

RFC 2389 *Feature negotiation mechanism for the File Transfer Protocol* P. Hethmon, R. Elz

RFC 2401 *Security Architecture for Internet Protocol* S. Kent, R. Atkinson

RFC 2402 *IP Authentication Header* S. Kent, R. Atkinson

RFC 2403 *The Use of HMAC-MD5–96 within ESP and AH* C. Madson, R. Glenn

RFC 2404 *The Use of HMAC-SHA–1–96 within ESP and AH* C. Madson, R. Glenn

RFC 2405 *The ESP DES-CBC Cipher Algorithm With Explicit IV* C. Madson, N. Doraswamy

RFC 2406 *IP Encapsulating Security Payload (ESP)* S. Kent, R. Atkinson

RFC 2407 *The Internet IP Security Domain of Interpretation for ISAKMP*D. Piper

RFC 2408 *Internet Security Association and Key Management Protocol (ISAKMP)* D. Maughan, M. Schertler, M. Schneider, J. Turner

RFC 2409 *The Internet Key Exchange (IKE)* D. Harkins, D. Carrel

RFC 2410 *The NULL Encryption Algorithm and Its Use With IPsec* R. Glenn, S. Kent,

RFC 2428 *FTP Extensions for IPv6 and NATs* M. Allman, S. Ostermann, C. Metz

RFC 2445 *Internet Calendaring and Scheduling Core Object Specification (iCalendar)* F. Dawson, D. Stenerson

RFC 2459 *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* R. Housley, W. Ford, W. Polk, D. Solo

RFC 2460 *Internet Protocol, Version 6 (IPv6) Specification* S. Deering, R. Hinden

RFC 2461 *Neighbor Discovery for IP Version 6 (IPv6)* T. Narten, E. Nordmark, W. Simpson

RFC 2462 *IPv6 Stateless Address Autoconfiguration* S. Thomson, T. Narten

RFC 2463 *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification* A. Conta, S. Deering

RFC 2464 *Transmission of IPv6 Packets over Ethernet Networks* M. Crawford

RFC 2466 *Management Information Base for IP Version 6: ICMPv6 Group* D. Haskin, S. Onishi

RFC 2476 *Message Submission* R. Gellens, J. Klensin

RFC 2487 *SMTP Service Extension for Secure SMTP over TLS* P. Hoffman

RFC 2505 *Anti-Spam Recommendations for SMTP MTAs* G. Lindberg

RFC 2523 *Photuris: Extended Schemes and Attributes* P. Karn, W. Simpson

RFC 2535 *Domain Name System Security Extensions* D. Eastlake 3rd

RFC 2538 *Storing Certificates in the Domain Name System (DNS)* D. Eastlake 3rd, O. Gudmundsson

RFC 2539 *Storage of Diffie-Hellman Keys in the Domain Name System (DNS)* D. Eastlake 3rd

RFC 2540 *Detached Domain Name System (DNS) Information* D. Eastlake 3rd

RFC 2554 *SMTP Service Extension for Authentication* J. Myers

RFC 2570 *Introduction to Version 3 of the Internet-standard Network Management Framework* J. Case, R. Mundy, D. Partain, B. Stewart

RFC 2571 *An Architecture for Describing SNMP Management Frameworks* B. Wijnen, D. Harrington, R. Presuhn

RFC 2572 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 2573 *SNMP Applications* D. Levi, P. Meyer, B. Stewart

RFC 2574 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* U. Blumenthal, B. Wijnen

RFC 2575 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* B. Wijnen, R. Presuhn, K. McCloghrie

RFC 2576 *Co-Existence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* R. Frye, D. Levi, S. Routhier, B. Wijnen

RFC 2578 *Structure of Management Information Version 2 (SMIv2)* K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2579 *Textual Conventions for SMIv2* K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2580 *Conformance Statements for SMIv2* K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2581 *TCP Congestion Control* M. Allman, V. Paxson, W. Stevens

RFC 2583 *Guidelines for Next Hop Client (NHC) Developers* R. Carlson, L. Winkler

RFC 2591 *Definitions of Managed Objects for Scheduling Management Operations* D. Levi, J. Schoenwaelder

RFC 2625 *IP and ARP over Fibre Channel* M. Rajagopal, R. Bhagwat, W. Rickard

RFC 2635 *Don't SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)* S. Hambridge, A. Lunde

RFC 2637 *Point-to-Point Tunneling Protocol* K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn

RFC 2640 *Internationalization of the File Transfer Protocol* B. Curtin

RFC 2665 *Definitions of Managed Objects for the Ethernet-like Interface Types* J. Flick, J. Johnson

RFC 2671 *Extension Mechanisms for DNS (EDNS0)* P. Vixie

RFC 2672 *Non-Terminal DNS Name Redirection* M. Crawford

RFC 2675 *IPv6 Jumbograms* D. Borman, S. Deering, R. Hinden

RFC 2710 *Multicast Listener Discovery (MLD) for IPv6* S. Deering, W. Fenner, B. Haberman

RFC 2711 *IPv6 Router Alert Option* C. Partridge, A. Jackson

RFC 2740 *OSPF for IPv6* R. Coltun, D. Ferguson, J. Moy

RFC 2753 *A Framework for Policy-based Admission Control* R. Yavatkar, D. Pendarakis, R. Guerin

RFC 2782 *A DNS RR for specifying the location of services (DNS SRV)* A. Gubrandsen, P. Vixix, L. Esibov

RFC 2821 *Simple Mail Transfer Protocol* J. Klensin, Ed.

RFC 2822 *Internet Message Format* P. Resnick, Ed.

RFC 2840 *TELNET KERMIT OPTION* J. Altman, F. da Cruz

RFC 2845 *Secret Key Transaction Authentication for DNS (TSIG)* P. Vixie, O. Gudmundsson, D. Eastlake 3rd, B. Wellington

RFC 2851 *Textual Conventions for Internet Network Addresses* M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 2852 *Deliver By SMTP Service Extension* D. Newman

RFC 2874 *DNS Extensions to Support IPv6 Address Aggregation and Renumbering* M. Crawford, C. Huitema

RFC 2915 *The Naming Authority Pointer (NAPTR) DNS Resource Record* M. Mealling, R. Daniel

RFC 2920 *SMTP Service Extension for Command Pipelining* N. Freed

RFC 2930 *Secret Key Establishment for DNS (TKEY RR)* D. Eastlake, 3rd

RFC 2941 *Telnet Authentication Option* T. Ts'o, ed., J. Altman

RFC 2942 *Telnet Authentication: Kerberos Version 5* T. Ts'o

RFC 2946 *Telnet Data Encryption Option* T. Ts'o

RFC 2952 *Telnet Encryption: DES 64 bit Cipher Feedback* T. Ts'o

RFC 2953 *Telnet Encryption: DES 64 bit Output Feedback* T. Ts'o

RFC 2992 *Analysis of an Equal-Cost Multi-Path Algorithm* C. Hopps

RFC 3019 *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol* B. Haberman, R. Worzella

RFC 3060 *Policy Core Information Model—Version 1 Specification* B. Moore, E. Ellesson, J. Strassner, A. Westerinen

RFC 3152 *Delegation of IP6.ARPA* R. Bush

RFC 3164 *The BSD Syslog Protocol* C. Lonvick

RFC 3207 *SMTP Service Extension for Secure SMTP over Transport Layer Security* P. Hoffman

RFC 3226 *DNSSEC and IPv6 A6 aware server/resolver message size requirements* O. Gudmundsson

RFC 3291 *Textual Conventions for Internet Network Addresses* M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 3363 *Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System* R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain

RFC 3376 *Internet Group Management Protocol, Version 3* B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan

RFC 3390 *Increasing TCP's Initial Window* M. Allman, S. Floyd, C. Partridge

RFC 3410 *Introduction and Applicability Statements for Internet-Standard Management Framework* J. Case, R. Mundy, D. Partain, B. Stewart

RFC 3411 *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* D. Harrington, R. Presuhn, B. Wijnen

RFC 3412 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 3413 *Simple Network Management Protocol (SNMP) Applications* D. Levi, P. Meyer, B. Stewart

RFC 3414 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* U. Blumenthal, B. Wijnen

RFC 3415 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* B. Wijnen, R. Presuhn, K. McCloghrie

RFC 3416 *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)* R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3417 *Transport Mappings for the Simple Network Management Protocol (SNMP)* R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3418 *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)* R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3419 *Textual Conventions for Transport Addresses* M. Daniele, J. Schoenwaelder

RFC 3484 *Default Address Selection for Internet Protocol version 6 (IPv6)* R. Draves

RFC 3493 *Basic Socket Interface Extensions for IPv6* R. Gilligan, S. Thomson, J. Bound, J. McCann, W. Stevens

RFC 3513 *Internet Protocol Version 6 (IPv6) Addressing Architecture* R. Hinden, S. Deering

RFC 3526 *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)* T. Kivinen, M. Kojo

RFC 3542 *Advanced Sockets Application Programming Interface (API) for IPv6* W. Richard Stevens, M. Thomas, E. Nordmark, T. Jinmei

RFC 3566 *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec* S. Frankel, H. Herbert

RFC 3569 *An Overview of Source-Specific Multicast (SSM)* S. Bhattacharyya, Ed.

RFC 3584 *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* R. Frye, D. Levi, S. Routhier, B. Wijnen

RFC 3602 *The AES-CBC Cipher Algorithm and Its Use with IPsec* S. Frankel, R. Glenn, S. Kelly

RFC 3629 *UTF-8, a transformation format of ISO 10646* R. Kermode, C. Vicisano

RFC 3658 *Delegation Signer (DS) Resource Record (RR)* O. Gudmundsson

RFC 3678 *Socket Interface Extensions for Multicast Source Filters* D. Thaler, B. Fenner, B. Quinn

RFC 3715 *IPsec-Network Address Translation (NAT) Compatibility Requirements* B. Aboba, W. Dixon

RFC 3810 *Multicast Listener Discovery Version 2 (MLDv2) for IPv6* R. Vida, Ed., L. Costa, Ed.

RFC 3947 *Negotiation of NAT-Traversal in the IKE* T. Kivinen, B. Swander, A. Huttunen, V. Volpe

RFC 3948 *UDP Encapsulation of IPsec ESP Packets* A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg

RFC 4001 *Textual Conventions for Internet Network Addresses* M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 4007 *IPv6 Scoped Address Architecture* S. Deering, B. Haberman, T. Jinmei, E. Nordmark, B. Zill

RFC 4022 *Management Information Base for the Transmission Control Protocol (TCP)* R. Raghunarayan

RFC 4106 *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)* J. Viega, D. McGrew

RFC 4109 *Algorithms for Internet Key Exchange version 1 (IKEv1)* P. Hoffman

RFC 4113 *Management Information Base for the User Datagram Protocol (UDP)* B. Fenner, J. Flick

RFC 4191 *Default Router Preferences and More-Specific Routes* R. Draves, D. Thaler

RFC 4217 *Securing FTP with TLS* P. Ford-Hutchinson

RFC 4292 *IP Forwarding Table MIB* B. Haberman

RFC 4293 *Management Information Base for the Internet Protocol (IP)* S. Routhier

RFC 4301 *Security Architecture for the Internet Protocol* S. Kent, K. Seo

RFC 4302 *IP Authentication Header* S. Kent

RFC 4303 *IP Encapsulating Security Payload (ESP)* S. Kent

RFC 4304 *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)* S. Kent

RFC 4306 *Internet Key Exchange (IKEv2) Protocol* C. Kaufman, Ed.

RFC 4307 *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)* J. Schiller

RFC 4308 *Cryptographic Suites for IPsec* P. Hoffman

RFC 4434 *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol* P. Hoffman

RFC 4552 *Authentication/Confidentiality for OSPFv3* M. Gupta, N. Melam

RFC 4678 *Server/Application State Protocol v1* A. Bivens

RFC 4718 *IKEv2 Clarifications and Implementation Guidelines* P. Eronen, P. Hoffman

RFC 4753 *ECP Groups for IKE and IKEv2* D. Fu, J. Solinas

RFC 4754 *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)* D. Fu, J. Solinas

RFC 4809	*Requirements for an IPsec Certificate Management Profile* C. Bonatti, Ed., S. Turner, Ed., G. Lebovitz, Ed.
RFC 4835	*Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header* V. Manral
RFC 4862	*IPv6 Stateless Address Autoconfiguration* S. Thomson, T. Narten, T. Jinmei
RFC 4868	*Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec* S. Kelly, S. Frankel
RFC 4869	*Suite B Cryptographic Suites for IPsec* L. Law, J. Solinas
RFC 4941	*Privacy Extensions for Stateless Address Autoconfiguration in IPv6* T. Narten, R. Draves, S. Krishnan
RFC 4945	*The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX* B. Korver
RFC 5014	*IPv6 Socket API for Source Address Selection* E. Nordmark, S. Chakrabarti, J. Laganier
RFC 5095	*Deprecation of Type 0 Routing Headers in IPv6* J. Abley, P. Savola, G. Neville-Neil
RFC 5175	*IPv6 Router Advertisement Flags Option* B. Haberman, Ed., R. Hinden
RFC 5282	*Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol* D. Black, D. McGrew

Internet drafts

Internet drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Other groups may also distribute working documents as Internet drafts. You can see Internet drafts at http://www.ietf.org/ID.html.

Several areas of IPv6 implementation include elements of the following Internet drafts and are subject to change during the RFC review process.

Draft Title and Author

draft-ietf-ipngwg-icmp-v3-07
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering

Appendix B. Accessibility

Publications for this product are offered in Adobe® Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library Web site or the z/OS Information Center. If you continue to experience problems, send an e-mail to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Mail Station P181
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer/Library Server versions of z/OS books in the Internet library at www.ibm.com/systems/z/os/zos/bkserv/.

Notices

This information was developed for products and services offered in the USA.

IBM may not offer all of the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not 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:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14 Shimotsuruma,, Yamato-Shi
Kanagawa 242-8502 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.

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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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_.

IBM is required to include the following statements in order to distribute portions of this document and the software described herein to which contributions have been made by The University of California. Portions herein © Copyright 1979, 1980, 1983, 1986, Regents of the University of California. Reproduced by permission. Portions herein were developed at the Electrical Engineering and Computer Sciences Department at the Berkeley campus of the University of California under the auspices of the Regents of the University of California.

Portions of this publication relating to RPC are Copyright © Sun Microsystems, Inc., 1988, 1989.

Some portions of this publication relating to X Window System** are Copyright © 1987, 1988 by Digital Equipment Corporation, Maynard, Massachusetts, and the Massachusetts Institute Of Technology, Cambridge, Massachusetts. All Rights Reserved.

Some portions of this publication relating to X Window System are Copyright © 1986, 1987, 1988 by Hewlett-Packard Corporation.

Permission to use, copy, modify, and distribute the M.I.T., Digital Equipment Corporation, and Hewlett-Packard Corporation portions of this software and its documentation for any purpose without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T., Digital, and Hewlett-Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T., Digital, and Hewlett-Packard make no representation about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright © 1983, 1995-1997 Eric P. Allman

Copyright © 1988, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

```
This product includes software developed by the University of
California, Berkeley and its contributors.
```

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software program contains code, and/or derivatives or modifications of code originating from the software program "Popper." Popper is Copyright ©1989-1991 The Regents of the University of California, All Rights Reserved. Popper was created by Austin Shelton, Information Systems and Technology, University of California, Berkeley.

Permission from the Regents of the University of California to use, copy, modify, and distribute the "Popper" software contained herein for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies. HOWEVER, ADDITIONAL PERMISSIONS MAY BE NECESSARY FROM OTHER PERSONS OR ENTITIES, TO USE DERIVATIVES OR MODIFICATIONS OF POPPER.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THE POPPER SOFTWARE, OR ITS DERIVATIVES OR MODIFICATIONS, AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE POPPER SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

Copyright © 1983 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to

endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   `This product includes software developed by the University of California, Berkeley and its contributors.`
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original M.I.T. software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

This product includes cryptographic software written by Eric Young.

Copyright © 1999, 2000 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 2004 IBM Corporation and its licensors, including Sendmail, Inc., and the Regents of the University of California. All rights reserved.

Copyright © 1999,2000,2001 Compaq Computer Corporation

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

You can obtain softcopy from the z/OS Collection (SK3T-4269), which contains BookManager and PDF formats.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are registered trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

Bibliography

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

z/OS Communications Server documentation is available in the following forms:

- Online at the z/OS Internet Library web page at www.ibm.com/systems/z/os/zos/bkserv/
- In softcopy on CD-ROM collections. See "Softcopy information" on page xvii.

z/OS Communications Server library updates

An index to z/OS Communications Server book updates is at http://www.ibm.com/support/docview.wss?uid=swg21178966. Updates to documents are also available on RETAIN® and in information APARs (info APARs). Go to http://www.ibm.com/software/network/commserver/zos/support to view information APARs. In addition, Info APARs for z/OS documents are in *z/OS and z/OS.e DOC APAR and PTF ++HOLD Documentation*, which can be found at http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/ BOOKS/ZIDOCMST/CCONTENTS.

z/OS Communications Server information

z/OS Communications Server product information is grouped by task in the following tables.

Planning

Title	Number	Description
z/OS Communications Server: New Function Summary	GC31-8771	This document is intended to help you plan for new IP for SNA function, whether you are migrating from a previous version or installing z/OS for the first time. It summarizes what is new in the release and identifies the suggested and required modifications needed to use the enhanced functions.
z/OS Communications Server: IPv6 Network and Application Design Guide	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
z/OS Communications Server: IP Configuration Guide	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 *z/OS Communications Server: IP Configuration Reference*.

Title	Number	Description
z/OS Communications Server: IP Configuration Reference	SC31-8776	This document presents information for people who want to administer and maintain IP. Use this document in conjunction with the *z/OS Communications Server: IP Configuration Guide*. The information in this document includes: • TCP/IP configuration data sets • Configuration statements • Translation tables • Protocol number and port assignments
z/OS Communications Server: SNA Network Implementation Guide	SC31-8777	This document presents the major concepts involved in implementing an SNA network. Use this document in conjunction with the *z/OS Communications Server: SNA Resource Definition Reference*.
z/OS Communications Server: SNA Resource Definition Reference	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 *z/OS Communications Server: SNA Network Implementation Guide*.
z/OS Communications Server: SNA Resource Definition Samples	SC31-8836	This document contains sample definitions to help you implement SNA functions in your networks, and includes sample major node definitions.
z/OS Communications Server: IP Network Print Facility	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
z/OS Communications Server: IP User's Guide and Commands	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.
z/OS Communications Server: IP System Administrator's Commands	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.
z/OS Communications Server: SNA Operation	SC31-8779	This document serves as a reference for programmers and operators requiring detailed information about specific operator commands.
z/OS Communications Server: Quick Reference	SX75-0124	This document contains essential information about SNA and IP commands.

Customization

Title	Number	Description
z/OS Communications Server: SNA Customization	SC31-6854	This document enables you to customize SNA, and includes the following: • Communication network management (CNM) routing table • Logon-interpret routine requirements • Logon manager installation-wide exit routine for the CLU search exit • TSO/SNA installation-wide exit routines • SNA installation-wide exit routines

Writing application programs

Title	Number	Description
z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference	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.
z/OS Communications Server: IP CICS Sockets Guide	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.
z/OS Communications Server: IP IMS Sockets Guide	SC31-8830	This document is for programmers who want application programs that use the IMS TCP/IP application development services provided by the TCP/IP Services of IBM.
z/OS Communications Server: IP Programmer's Guide and Reference	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.
z/OS Communications Server: SNA Programming	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.
z/OS Communications Server: SNA Programmer's LU 6.2 Guide	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.)
z/OS Communications Server: SNA Programmer's LU 6.2 Reference	SC31-8810	This document provides reference material for the SNA LU 6.2 programming interface for host application programs.
z/OS Communications Server: CSM Guide	SC31-8808	This document describes how applications use the communications storage manager.

Title	Number	Description
z/OS Communications Server: CMIP Services and Topology Agent Guide	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
z/OS Communications Server: IP Diagnosis Guide	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.
z/OS Communications Server: ACF/TAP Trace Analysis Handbook	GC23-8588-00	This document explains how to gather the trace data that is collected and stored in the host processor. It also explains how to use the Advanced Communications Function/Trace Analysis Program (ACF/TAP) service aid to produce reports for analyzing the trace data information.
z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures and *z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT*	GC31-6850 GC31-6851	These documents help you identify an SNA problem, classify it, and collect information about it before you call the IBM Support Center. The information collected includes traces, dumps, and other problem documentation.
z/OS Communications Server: SNA Data Areas Volume 1 and *z/OS Communications Server: SNA Data Areas Volume 2*	GC31-6852 GC31-6853	These documents describe SNA data areas and can be used to read an SNA dump. They are intended for IBM programming service representatives and customer personnel who are diagnosing problems with SNA.

Messages and codes

Title	Number	Description
z/OS Communications Server: SNA Messages	SC31-8790	This document describes the ELM, IKT, IST, IUT, IVT, and USS messages. Other information in this document includes: • Command and RU types in SNA messages • Node and ID types in SNA messages • Supplemental message-related information
z/OS Communications Server: IP Messages Volume 1 (EZA)	SC31-8783	This volume contains TCP/IP messages beginning with EZA.
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	SC31-8784	This volume contains TCP/IP messages beginning with EZB or EZD.
z/OS Communications Server: IP Messages Volume 3 (EZY)	SC31-8785	This volume contains TCP/IP messages beginning with EZY.
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	SC31-8786	This volume contains TCP/IP messages beginning with EZZ and SNM.
z/OS Communications Server: IP and SNA Codes	SC31-8791	This document describes codes and other information that appear in z/OS Communications Server messages.

Index

Numerics

4301 compliance, IBM Health Checker for z/OS RFC 92

A

ACB sharing, Telnet LU 34
accelerator, QDIO routing 74
accelerator, sysplex distributor connection routing 76
accept_and_recv socket API 69
accessibility 117
ACF/SSP 91
ACF/TAP 91
adaptive rate-based (ARB) flow control algorithm, progressive-mode 87
address autoconfiguration, IPv6 stateless 64
address selection policy table 26
address selection, IPv6 socket API for source 26
Advanced Communications Function/Trace Analysis Program (ACF/TAP) 91
AES algorithm 38
agent, VTAM topology 11
algorithm, progressive-mode adaptive rate-based (ARB) flow control 87
algorithms, WLM routing 68
analyzer data, OSA network traffic 94
APAR OA26490 88
API to obtain IPv4 network interface MTU 66
API, accept_and_recv socket 69
appliances, IBM WebSphere DataPower 32, 77
application definition, dynamic 86
applications, tier 1 and tier 2 76
APPN
  default COS 12
  default transmission groups 12
APPN topology database update (TDU) processing 90
archival of z/OS UNIX files 82
AT-TLS enhancements 80
AT-TLS performance 33
autoconfiguration, IPv6 stateless address 64

B

balancing, workload 32, 77
banner for otelnetd, pre-logon 63
BIND 4.9.3 DNS server support 53
BIND9 DNS server 85
BINL support 53
browser and search facilities, syslogd 82
buffer size 70
building dynamic application definition 86
bulk data, streaming 29
bundles, hash and URL encoding 36

C

cache, resolver DNS 73
callable NMI (EZBNMIFR) GetConnectionDetail request, TCP/IP 46
Callable NMI, GetProfile request for the TCP/IP 92
catalog synchronization, Netstat 51
certificate bundles, hash and URL encoding 36
certificate revocation lists, certificate trust chains 37
certificate services for XML appliances 72
certificate trust chains and certificate revocation lists 37
check, migration health 92
checks, IBM Health Checker for z/OS 42
CHPID types 31
CICS sockets interface and listener 67
client for sending Internet mail, SMTP 54
code page, EBCDIC 83
commands, z/OS UNIX shell 85
common storage area (ECSA) usage 34
Communications Server for z/OS, online information xix
compliance, IBM Health Checker for z/OS RFC 4301 92
Configuration Assistant enhancements 81
configuration data, stack 92
connection health verification for EE 44
connection isolation 97
connection routing accelerator, sysplex distributor 76
connection routing, sysplex distributor 28
connection, trusted TCP 40
connections in SynRcvd state, TCP 53
console support, MVS 85
COSAPPN file 12
cryptographic currency 38
cryptographic mode, IPSec support for FIPS 140 39
CSM ECSA storage relief 67
CSM usage statistics 93
CSSMTP 54
CSSMTP management 47
CSVDYLPA 70, 71
CV64 function 49

D

daemon browser application, ISPF-based syslog 82
data sets, distribution library 4
data space VIT with INOP dump 86
data tracing (DATTRACE) 49
data, streaming bulk 29
database update (TDU) processing, APPN topology 90
DataPower appliances, IBM WebSphere 32, 77
DCAS MODIFY command 41
deadlock caused by insufficient TCP receive buffer size 70
debug level, modifying 41
definition, dynamic application 86
delayed TCP acknowledgements, traffic stalls caused by Nagle algorithms 70
deprecation of IPv6 type 0 route header 66
detection and recovery, sysplex 35
DHCP support 53
disability 117
DISPLAY MODELS command 86
DISPLAY NET,TOPO,LIST=TDUDIAG command 45
DISPLAY TCPIP,,STOR command 51
displaying FTP space statistics for volumes 61
DISTMETHOD SERVERWLM statement 68
distribution library data sets 4
DLC layer, forwarding at the 74
DNS cache, resolver 73

DNS name servers and resolver support 27
DNS name servers, resolver reaction to unresponsive 34
DNS server, BIND9 85
DNS, online information xx
domain name servers 53
dropping TCP connections 42
dump processing, VTAM INOP 86
DVIPA information provided by EZBNMIFR 95
DVIPAs in MOVING state 68
dynamic application definition 86

E

EBCDIC code page support 83
echo reply packets, displaying 96
ECSA storage constraint relief, 71
ECSA storage relief 67
ECSA usage 34
EE connection health verification 44
EEVERIFY start option 44
encoding of certificates and certificate bundles, hash and URL 36
encryption features 2
Enterprise Extender and multipath 45
Enterprise Extender IPSec performance improvements 72
event record, SMF 119 92
execution server, MVS remote 63
extended common storage area (ECSA) usage 34
EZACMD command 85
EZBNMIFR 46
EZBNMIFR and request types 95

F

fast local sockets 34
fast local sockets for TCP connections 34
files, archival of z/OS UNIX 82
FIPS 140 cryptographic mode, IPSec support 39
firewall 61
flow control algorithm, progressive-mode adaptive rate-based (ARB) 87
formatting trace information 91
forwarding at the DLC layer 74
FTP access to UNIX named pipes 56
FTP passive mode 61
FTP reports 61
FWFRIENDLY parameter 62

G

GetConnectionDetail request 46
GetProfile request 92
GetProfile request for the TCP/IP Callable NMI 92
GLOBALCONFIG profile statement, WLMPRIORITYQ parameter 96

H

hash and URL encoding of certificates and certificate bundles 36
Health Checker for z/OS migration health check, z/OS 85
Health Checker for z/OS OMPROUTE checks 42
Health Checker for z/OS RFC 4301 compliance, IBM 92
health of a server application 74
health verification of connections 44
HFS (hierarchical file system) parts for z/OS Communications Server 4
high latency networks 71
high performance routing (HPR) performance 87
HiperSockets and routing acceleration 74
HiperSockets, storage conditions 67
hot-standby server and sysplex distributor support 33

I

IBM Health Checker for z/OS 42
IBM Health Checker for z/OS OMPROUTE checks 42
IBM Health Checker for z/OS RFC 4301 compliance 92
IBM Software Support Center, contacting xiii
IBM WebSphere DataPower appliances 32, 77
IBMTGPS file (APPN) 12
IKE daemon's retransmission scheme 79
IKE version 2 36
IKEv2 support 35
ILWEIGHTING parameter 68
inbound packets, forwarding 74
inbound workload queueing 29
Information APARs xvii
INOP dump processing 86
interface isolation, QDIO support for OSA 97
Internet mail, SMTP client for sending 54
Internet, finding z/OS information online xix
intraensemble data network 31
intranode management network 31
IPSec enhancements 79
IPSec performance improvements, Enterprise Extender 72
IPSec support for certificate trust chains and certificate revocation lists 37
IPSec support for cryptographic currency 38
IPSec support for FIPS 140 cryptographic mode 39
IPv4 network interface MTU 66
IPv6 addresses, temporary 64
IPv6 connections to DNS name servers and resolver support 27
IPv6 router advertisement 25
IPv6 socket API for source address selection 26
IPv6 stateless address autoconfiguration 64
IPv6 type 0 route header, RFC 5095 deprecation 66
IPV6_RTHDR option 66
isolation, QDIO support for OSA interface 97
ISPF-based syslog daemon browser application 82

J

joining the sysplex XCF group 43

K

keyboard 117
KeyID identity type 35

L

latency mode, OSA-Express3 optimized 78
license, patent, and copyright information 119
load modules 70
log messages, processing of 82
LOGONHERE parameter 64
LookAt xvii
LU ACB sharing, Telnet 34

M

mail, SMTP client for sending Internet 54
mainframe
  education xvii
mapping of Workload Manager (WLM) service classes to outbound Queued Direct I/O (QDIO) priorities 96
message catalog synchronization, Netstat 51
message transfer agent (MTA), target 54
messages, processing of log 82
migration health check 92
migration health check, z/OS Health Checker for z/OS 85
MODIFY command, DCAS 41
MOVING DVIPAs 68
msg_waitall 70
MTA (target message transfer agent) 54
MTU, API to obtain IPv4 network interface 66
multi-tier z/OS workloads, sysplex distributor optimization 76
Multipath for Enterprise Extender 45
MULTIPATH statement 45
MULTPATH start option 45
MVS console support 85
MVS data sets 4
MVS remote execution server 63
MVS, installing VTAM under 7

N

Nagle algorithms and delayed TCP acknowledgements 70
name servers, DNS 27
name servers, unresponsive DNS 34
named pipes, FTP access to UNIX 56
NAT firewall 61
NDB support 53
Netstat message catalog synchronization 51
Netstat report 53
network interface MTU 66
network management interface and detailed CSM usage 93
network traffic analyzer data, OSA 94
NMI (EZBNMIFR) GetConnectionDetail request 46
NMI Enhancements
  interface and device statistics 46
  sysplex event using NMI real-time SMF event 47
NMI storage statistics 51
NMI, GetProfile request for the TCP/IP Callable 92
NSS private key and certificate services for XML appliances 72
NSS processing of IPSec certificate trust chains and certificate revocation lists 37

O

O/S data sets used by VTAM 7
OA26490, APAR 88
OMPROUTE 53
OMPROUTE checks, IBM Health Checker for z/OS 42
OMPROUTE processing 67
optimization for multi-tier z/OS workloads, sysplex distributor 76
optimized latency mode, OSA-Express3 78
OPTLOCAL 76
OSA interface isolation 97
OSA network traffic analyzer data 94
OSA-Express in QDIO mode 29
OSA-Express in QDIO mode, storage conditions 67
OSA-Express QDIO and routing acceleration 74
OSA-Express3 adapters 31
OSA-Express3 optimized latency mode 78
OSM and OSX CHPID types 31
OSPF 53
otelnetd 63
ownership statistics, storage 93

P

packet flow between OSA devices 97
packet tracing 50
packets, echo reply 96
packets, forwarding 74
PASSIVEIGNOREADDR configuration option 61
PASV reply 61
path switches 87
pathlength, TCP/IP 70
Ping command, displaying echo details 96
pipe stalls, RTP 45
pipes, FTP access to UNIX named 56
planning checklist 3
Policy Agent, monitoring applications 83
policy table, address selection 26
pre-logon banner for otelnetd 63
prerequisite information xvii
priorities and mapping 96
problem detection and recovery, sysplex 35
processing of log messages and syslogd 82
processing, APPN topology database update (TDU) 90
PROCXCOST parameter 68
progressive-mode adaptive rate-based (ARB) flow control algorithm 87

Q

QDIO mode, OSA-Express 67
QDIO mode, OSA-Express traffic 29
QDIO routing accelerator 74
QDIO support for OSA interface isolation 97
QDISK parameter 61
Queued Direct I/O (QDIO) priorities, mapping 96
queueing, inbound workload 29

R

read call() 70
real time trace collection 94
recovery, sysplex 35
reduce extended common storage area (ECSA) usage 34
release considerations in V1R11 53
remote execution server, MVS 63
resolver DNS cache 73
resolver queries 53
resolver reaction to unresponsive DNS name servers 34
resolver support for IPv6 connections to DNS name servers 27
revocation lists, certificate trust chains 37
RFC (request for comments) 99
  accessing online xix
RFC 2408 79
RFC 3484 26
RFC 4191 25
RFC 4301 compliance, IBM Health Checker for z/OS 92
RFC 4941 64
RFC 5014 26
RFC 5095 66

RFC 5175 25
router advertisement, IPv6 25
routing 53
routing accelerator, QDIO 74
routing accelerator, sysplex distributor connection 76
routing algorithms, WLM 68
routing, sysplex distributor connection 28
RSHD server 63
RTP pipe stalls 45

S

sending Internet mail 54
server efficiency factor (SEF) 74
SERVERWLM statement, DISTMETHOD 68
service classes to outbound Queued Direct I/O (QDIO) priorities, mapping of Workload Manager (WLM) 96
session manager 49
SetSockOpt call, TCP_NODELAY 70
SHAREACB statement 34
shell commands, z/OS UNIX 85
shortcut keys 117
SIOCGIFMTU ioctl 66
SMF 119 event record 92
SMF 119 event records 47
SMF 119 record subtypes 47
SMTP client for sending Internet mail 54
SMTPD 54
SNMP Manager API 51
socket data flow start and end 49
sockets, fast local 34
softcopy information xvii
space statistics for volumes, FTP 61
SRCIP configuration statement 26
stack configuration data 92
stalls caused by Nagle algorithms and delayed TCP acknowledgements 70
stalls, RTP pipe 45
stateless address autoconfiguration, IPv6 64
statistics for volumes, FTP 61
statistics, storage ownership 93
storage area usage 34
storage constraint relief, 71
storage ownership statistics 93
storage shortage and relief 67
storage statistics 51
streaming bulk data 29
support considerations in V1R11 53
support for OSA interface isolation, QDIO 97
switches, path 87
synchronization, Netstat message catalog 51
SynRcvd state, TCP connections in 53
syntax diagram, how to read xiv
syslogd browser and search facilities 82
syslogd enhancements 82
sysplex distributor 75
sysplex distributor connection routing 28
sysplex distributor connection routing accelerator 76
sysplex distributor optimization for multi-tier z/OS workloads 76
sysplex distributor support for DataPower 32, 77
sysplex distributor support for hot-standby server 33
sysplex distributor workload balancing 32, 77
sysplex event notification 47
sysplex event using NMI real-time SMF event 47
sysplex problem detection and recovery 35
sysplex XCF group, joining 43

T

target message transfer agent (MTA) 54
TCP acknowledgements, Traffic stalls caused by Nagle algorithms 70
TCP connection, trusted 40
TCP connections in SynRcvd state 53
TCP connections, dropping 42
TCP receive buffer size 70
TCP throughput improvements 71
TCP_NODELAY SetSockOpt call 70
TCP/IP
  online information xix
  protocol specifications 99
TCP/IP callable NMI (EZBNMIFR) GetConnectionDetail request 46
TCP/IP pathlength 70
TCPSTACKSOURCEVIPA 68
TDU processing 90
Technotes xvii
Telnet LU ACB sharing 34
TEMPADDRS parameter 65
temporary addresses 64
throughput improvements, TCP 71
tier 1 and tier 2 server applications 76
TN3270E server 41
TN3270E server and session manager 49
topology agent 11
topology agent, enabling 7
topology database diagnostics 45
topology database update (TDU) processing, APPN 90
trace collection, real time 94
trace information 91
trace resolver 73
trace resolver output 53
tracing packets 50
trademark information 127
traffic analyzer data, OSA network 94
traffic stalls 70
transmission groups (TG), APPN default 12
trust chains and certificate revocation lists 37
trusted TCP connection 40
tuning window size 71
type 0 route header, RFC 5095 deprecation of IPv6 66

U

UNIX files, archival of z/OS 82
UNIX named pipes 56
UNIX shell commands 85
UNRESPONSIVETHRESHOLD configuration statement 35

V

VARY TCPIP,,DROP command 42
Verbose Ping 96
virtual storage constraint relief 71
VIT with INOP dump, data space 86
volumes, FTP reports 61
VTAM INOP dump processing 86
VTAM topology agent 11
VTAM topology agent, enabling 7
VTAM, online information xix

W

window size, tuning 71
WLM routing algorithms 68
WLMPRIORITYQ parameter 96
workload balancing 32, 77
Workload Manager (WLM) service classes to outbound Queued Direct I/O (QDIO) priorities 96
workload performance and OSA-Express3 optimized latency mode 78
workload queueing, inbound 29
workload, zIIP or zAAP targeted 68
workloads, sysplex distributor optimization for multi-tier z/OS 76

X

XCF group, joining 43
XML appliances 72

Z

z/OS Basic Skills information center xvii
z/OS Basic Skills Information Center xvii
z/OS Health Checker for z/OS migration health check 85
z/OS UNIX shell commands 85
z/OS V1R11 Communications Server release summary 53
z/OS V1R12 Communications Server release summary 25
z/OS workloads, sysplex distributor optimization for multi-tier 76
z/OS, documentation library listing 129
zIIP or zAAP targeted workload 68
zSeries, definition of 1
zSystem, 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.

Please send your comments to us in either of the following ways:

- If you prefer to send comments by FAX, use this number: 1+919-254-1258
- If you prefer to send comments electronically, use this address:
  - comsvrcf@us.ibm.com
- If you prefer to send comments by post, use this address:

```
International Business Machines Corporation
Attn: z/OS Communications Server Information Development
P.O. Box 12195, 3039 Cornwallis Road
Department AKCA, Building 501
Research Triangle Park, North Carolina 27709-2195
```

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.

Program Number: 5694–A01

Printed in USA

GC31-8771-06

Spine information:

z/OS Communications Server

z/OS V1R12.0 Comm Svr: New Function Summary

Version 1
Release 12