z/OS Communications Server

New Function Summary

Version 2 Release 1

GC27-3664-03

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

This edition applies to Version 2 Release 1 of z/OS (5650-ZOS), and to subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments. You can send us comments electronically by using one of the following methods:

Internet email:
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, and telephone number. Make sure to include the following information 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
Prerequisite and related information xiv

Summary of changes xix
Changes made in z/OS Version 2 Release 1, as updated February 2015 xix
Changes made in z/OS Version 2 Release 1, as updated September 2014 xix
Changes made in z/OS Version 2 Release 1, as updated December 2013 xix
Summary of changes for z/OS Version 2 Release 1 xix

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 V2R1 Communications Server 11
Data sets containing information for NCP 19

Chapter 2. Roadmap to functions 23

Chapter 3. V2R1 new function summary 27
Support considerations in V2R1 27
Security 27
Enhanced IDS IP fragment attack detection 28
Improve auditing of NetAccess rules 28
AT-TLS support for TLS v1.2 and related features 28
Improved FIPS 140 diagnostics 30
Limit defensive filter logging 30
QDIO outbound flood prevention 31
TN3270 client-bound data queueing limit 32
| AT-TLS enablement for DCAS 32
| Network security enhancements for SNMP 33
| TLS security enhancements for sendmail 34
| TLS security enhancements for Policy Agent 35
Simplification 35
Configuration Assistant performance improvements and enhanced user interface 36
Improve translation of special characters in linemode for TSO/VTAM 36
Resolver initialization resiliency 36
Enterprise Extender IPv6 address configuration 37
Simplified configuration for progressive mode ARB 38
Check TCP/IP profile syntax without applying configuration changes 39

User control of Ephemeral Port Ranges . . . 40
IPv4 INTERFACE statement for HiperSockets and Static VIPAs . . . 41
IBM Health Checker for z/OS GATEWAY statement . . . 43
IBM Health Checker for z/OS legacy device types . . . 43
CSSMTP mail message date header handling option . . . 44
Availability . . . 44
Socket establishment time for Netstat ALL/-A . . . 45
Sysplex-wide security associations for IPv6 . . . 45
HPR PSRETRY Enhancement . . . 46
RPCBIND recycle notification . . . 46
SNA serviceability enhancements . . . 47
TCP/IP serviceability enhancements . . . 47
Application, middleware, and workload enablement . . . 48
API to locate SYSLOGD configuration file . . . 48
Real-time application-controlled TCP/IP trace NMI . . . 48
FTP client security user exits . . . 49
Simplify FTP transfer of data sets between z/OS systems . . . 50
Enable DHCP clients on OSA interfaces . . . 51
NMI and SMF enhancements for TCP/IP applications . . . 51
Economics and platform efficiency . . . 53
QDIO acceleration coexistence with IP filtering . . . 53
TCP support for selective acknowledgments . . . 54
Shared Memory Communications over Remote Direct Memory Access . . . 55
DISPLAY NET, BRFUSE command Enhancement . . . 57
Shared Memory Communications over RDMA adapter (RoCE) virtualization . . . 57
Connection termination notification for sockets . . . 58
IPv6 support for policy-based routing . . . 59
Affinity for application-instance DVIPAs . . . 60
Enhanced Fast Path socket support . . . 60
Enhanced TCP protocol configuration options and default settings . . . 60

Chapter 4. V1R13 new function summary . . . 63
Support considerations in V1R13 . . . 63
Security . . . 63
Expanded intrusion detection services . . . 63
Network address translation traversal support for IKE version 2 . . . 64
Sysplex-Wide Security Associations for IKE version 2 . . . 65
Improved security granularity for VIPARANGE DVIPAs . . . 66
FTP support for password phrases . . . 67
Removed superuser requirement for Policy Agent and IKE daemon . . . 68
Enhanced IPsec support for FIPS 140 cryptographic mode . . . 69
Simplification . . . 69
Configuration Assistant management of multiple z/OS Communications Server releases . . . 70
Configuration Assistant discovery of stack IP addresses . . . 70
Configuration Assistant common configuration of multiple stacks . . . 72
Configuration Assistant enhancements . . . 73
Wildcard support for the PORTRANGE statement . . . 74
Dynamic infrastructure . . . 74
HiperSockets optimization for intraensemble data networks . . . 74
Support for additional VLANs for an OSA-Express QDIO port . . . 75
Economics and platform efficiency . . . 76
Increased CTRACE and VIT capacity . . . 76
OSA-Express4S QDIO IPv6 checksum and segmentation offload . . . 78
Availability . . . 79
System resolver autonomic quiescing of unresponsive name servers . . . 79
Improved convergence for sysplex distribution routing when joining a sysplex . . . 80
CSSMTP extended retry . . . 80
Monitor CSM constrained conditions for sysplex autonomics . . . 81
Application, middleware, and workload enablement . . . 81
Enhanced FTP support for extended address volumes . . . 82
FTP support for large-format data sets . . . 82

NMI for retrieving system resolver configuration information 83
Simplified authorization requirements for real-time TCP/IP network monitoring NMI 83
Enhancements to the TN3270E server 84
CSSMTP enhancements 85
Support for bypassing host name lookup in otelnetd 85
TCP/IP serviceability enhancements 86
SNA and Enterprise Extender 86
Intrusion detection services support for Enterprise Extender 87
Enterprise Extender firewall-friendly connectivity test 87
HPR packet trace analyzer for Enterprise Extender 88
Improved APPN routing resilience 88
Performance improvements for Enterprise Extender traffic 88

Appendix A. Related protocol specifications 91

Appendix B. Architectural specifications 115

Appendix C. Accessibility 117

Notices 119
Policy for unsupported hardware 127
Trademarks 127

Bibliography 129

Index 133

Communicating your comments to IBM 137

Figures

1. Correlation between DD statement and NCP definition statement 20

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 . . . 10
7. IBM-supplied default values for CSM buffer pools . . . 15
8. Roadmap to functions . . . 23
9. Enhanced IDS IP fragment attack detection . . . 28
10. Improve auditing of NetAccess rules . . . 28
11. AT-TLS support for TLS v1.2 and related features . . . 29
12. Improved FIPS 140 diagnostics . . . 30
13. Limit defensive filter logging. . . . 31
14. TN3270 client-bound data queueing limit . . . 32
15. AT-TLS enablement for DCAS . . . 32
16. Network security enhancements for SNMP . . . 34
17. TLS security enhancements for sendmail . . . 34
18. TLS security enhancements for Policy Agent . . . 35
19. Improve translation of special characters in linemode for TSO/VTAM . . . 36
20. Resolver initialization resiliency . . . 37
21. PTFs for APAR OA38234 . . . 37
22. Enterprise Extender IPv6 address configuration . . . 38
23. Simplified configuration for progressive mode ARB . . . 39
24. Check TCP/IP profile syntax without applying configuration changes . . . 40
25. User control of Ephemeral Port Ranges . . . 40
26. IPv4 INTERFACE statement for HiperSockets and Static VIPAs . . . 41
27. IBM Health Checker for z/OS migration check support . . . 43
28. IBM Health Checker for z/OS legacy device types . . . 44
29. CSSMTP mail message Date header handling option . . . 44
30. Obtain the start time of the connection . . . 45
31. Sysplex-wide security associations for IPv6 . . . 46
32. HPR PSRETRY Enhancement. . . . 46
33. RPCBIND recycle notification . . . 47
34. API to locate SYSLOGD configuration file . . . 48
35. Real-time application-controlled TCP/IP trace NMI . . . 49
36. FTP client security user exits . . . 50
37. Simplify FTP transfer of data sets between z/OS systems . . . 51
38. Enable DHCP clients on OSA interfaces . . . 51
39. NMI and SMF enhancements for TCP/IP applications about FTP daemon configuration data . . . 52
40. NMI and SMF enhancements for TCP/IP applications about TN3270 server profile configuration data 53
41. QDIO acceleration coexistence with IP filtering. . . . 54
42. TCP support for selective acknowledgments . . . 54
43. Shared Memory Communications over Remote Direct Memory Access . . . 55
44. Shared Memory Communications over RDMA Enhancements . . . 57
45. Shared Memory Communications over RDMA adapter (RoCE) virtualization . . . 58
46. Connection termination notification for sockets . . . 59
47. IPv6 policy-based routing . . . 59
48. Affinity for application-instance DVIPAs . . . 60
49. Enhanced TCP protocol configuration options and default settings . . . 61
50. Expanded intrusion detection services. . . . 64
51. Network address translation traversal support for IKE version 2 . . . 65
52. Sysplex-Wide Security Associations for IKE version 2 . . . 66
53. Improved security granularity for VIPARANGE DVIPAs . . . 66
54. FTP support for password phrases . . . 68
55. Removed superuser requirement for Policy Agent and IKE daemon . . . 68

56. Enhanced IPsec support for FIPS 140 cryptographic mode 69
57. Configuration Assistant management of multiple z/OS Communications Server releases 70
58. Configuration Assistant discovery of stack IP addresses 70
59. Configuration Assistant common configuration of multiple stacks 73
60. Configuration Assistant enhancements 74
61. Wildcard support for the PORTRANGE statement 74
62. HiperSockets optimization for intraensemble data networks 75
63. Support for additional VLANs for an OSA-Express QDIO port 76
64. Increased CTRACE and VIT capacity 77
65. OSA-Express4S QDIO IPv6 checksum and segmentation offload 78
66. System resolver autonomic quiescing of unresponsive name servers. 80
67. CSSMTP extended retry 81
68. Monitor CSM constrained conditions for sysplex autonomics 81
69. Enhanced FTP support for extended address volumes 82
70. FTP support for large-format data sets 83
71. NMI for retrieving system resolver configuration information 83
72. Simplified authorization requirements for real-time TCP/IP network monitoring NMI 84
73. Enhancements to the TN3270E server 84
74. CSSMTP enhancements 85
75. Support for bypassing host name lookup in otelnetd 86
76. TCP/IP serviceability enhancements 86
77. Intrusion detection services support for Enterprise Extender 87
78. Enterprise Extender firewall-friendly connectivity test 87
79. HPR packet trace analyzer for Enterprise Extender 88
80. Performance improvements for Enterprise Extender traffic 89

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 2 Release 1 Communications Server (z/OS Communications Server). It also includes the exploitation considerations of z/OS V1R13 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, 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 23 provides a roadmap of the functional enhancements introduced in z/OS V2R1 Communications Server and z/OS V1R13 Communications Server. Each entry indicates whether enabling or actions are required.
- Chapter 3, “V2R1 new function summary,” on page 27 summarizes the functions and migration considerations of z/OS V2R1 Communications Server.
- Chapter 4, “V1R13 new function summary,” on page 63 summarizes the functions and migration considerations of z/OS V1R13 Communications Server.
- Appendix A, “Related protocol specifications,” on page 91 lists the related protocol specifications for TCP/IP.
- Appendix B, “Architectural specifications,” on page 115 lists documents that provide architectural specifications for the SNA Protocol.
- Appendix C, “Accessibility,” on page 117 describes accessibility features to help users with physical disabilities.
- “Notices” on page 119 contains notices and trademarks used in this document.
- “Bibliography” on page 129 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 2 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 website: http://www.software.ibm.com/network/commserver/support/

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

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

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

If you would like to provide feedback on this publication, see "Communicating your comments to IBM" on page 137.

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.

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

- RDMA network interface card (RNIC), which is used to refer to the IBM® 10GbE RoCE Express® feature.
- Shared RoCE environment, which means that the 10GbE RoCE Express feature operates on an IBM z13™ (z13) or later system, and that the feature can be used

concurrently, or shared, by multiple operating system instances. The RoCE Express feature is considered to operate in a shared RoCE environment even if you use it with a single operating system instance.

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

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

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 collection.

Titles	Order Number	Description
IBM System z Redbooks Collection	SK3T-7876	The IBM Redbooks® publications selected for this CD series are taken from the IBM Redbooks inventory of over 800 books. All the Redbooks publications that are of interest to the System z® platform professional are identified by their authors and are included in this collection. The System z subject areas range from e-business application development and enablement to hardware, networking, Linux, solutions, security, parallel sysplex, and many others. For more information about the Redbooks publications, see http://www-03.ibm.com/systems/z/os/zos/zfavorites/.

Other documents

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

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

To find the complete z/OS library, visit the z/OS library in IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

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

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

Title	**Number**
DNS and BIND, Fifth Edition, O'Reilly Media, 2006	ISBN 13: 978-0596100575
Routing in the Internet, Second Edition, Christian Huitema (Prentice Hall 1999)	ISBN 13: 978-0130226471
sendmail, Fourth Edition, Bryan Costales, Claus Assmann, George Jansen, and Gregory Shapiro, O'Reilly Media, 2007	ISBN 13: 978-0596510299
SNA Formats	GA27-3136
TCP/IP Illustrated, Volume 1: The Protocols, W. Richard Stevens, Addison-Wesley Professional, 1994	ISBN 13: 978-0201633467
TCP/IP Illustrated, Volume 2: The Implementation, Gary R. Wright and W. Richard Stevens, Addison-Wesley Professional, 1995	ISBN 13: 978-0201633542
TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols, W. Richard Stevens, Addison-Wesley Professional, 1996	ISBN 13: 978-0201634952
TCP/IP Tutorial and Technical Overview	GG24-3376
Understanding LDAP	SG24-4986
z/OS Cryptographic Services System SSL Programming	*SC14-7495*
z/OS IBM Tivoli Directory Server Administration and Use for z/OS	*SC23-6788*
z/OS JES2 Initialization and Tuning Guide	*SA32-0991*
z/OS Problem Management	*SC23-6844*
z/OS MVS Diagnosis: Reference	*GA32-0904*
z/OS MVS Diagnosis: Tools and Service Aids	*GA32-0905*
z/OS MVS Using the Subsystem Interface	*SA38-0679*
z/OS V2R1 Program Directory	*GI11-9848*
z/OS UNIX System Services Command Reference	*SA23-2280*
z/OS UNIX System Services Planning	*GA32-0884*
z/OS UNIX System Services Programming: Assembler Callable Services Reference	*SA23-2281*
z/OS UNIX System Services User's Guide	*SA23-2279*
z/OS XL C/C++ Runtime Library Reference	*SC14-7314*
zEnterprise System and System z10 OSA-Express Customer's Guide and Reference	*SA22-7935*

Redbooks publications

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

Title	Number
IBM z/OS V2R1 Communications Server TCP/IP Implementation, Volume 1: Base Functions, Connectivity, and Routing	SG24-8096
IBM z/OS V2R1 Communications Server TCP/IP Implementation, Volume 2: Standard Applications	SG24-8097
IBM z/OS V2R1 Communications Server TCP/IP Implementation, Volume 3: High Availability, Scalability, and Performance	SG24-8098
IBM z/OS V2R1 Communications Server TCP/IP Implementation, Volume 4: Security and Policy-Based Networking	SG24-8099
IBM Communication Controller Migration Guide	SG24-6298
IP Network Design Guide	SG24-2580
Managing OS/390 TCP/IP with SNMP	SG24-5866
Migrating Subarea Networks to an IP Infrastructure Using Enterprise Extender	SG24-5957
SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements	SG24-5631
SNA and TCP/IP Integration	SG24-5291
TCP/IP in a Sysplex	SG24-5235
TCP/IP Tutorial and Technical Overview	GG24-3376
Threadsafe Considerations for CICS	SG24-6351

Where to find related information on the Internet

z/OS

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

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

z/OS Internet Library

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

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 publications, 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

Tivoli NetView for z/OS

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

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

RFCs

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

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

Internet drafts

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

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

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

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

DNS websites

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

USENET news groups
comp.protocols.dns.bind

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

BIND Users

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

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

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

The z/OS Basic Skills Information Center

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

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

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

To access the z/OS Basic Skills Information Center, open your web browser to the following website, which is available to all users (no login required):
http://www-01.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zbasics/homepage.html

Summary of changes

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

Changes made in z/OS Version 2 Release 1, as updated February 2015

This document contains information previously presented in z/OS Communications Server: New Function Summary, GC27-3664-02, which supported z/OS Version 2 Release 1.

Changes made in z/OS Version 2 Release 1, as updated September 2014

This document contains information previously presented in z/OS Communications Server: New Function Summary, GC27-3664-01, which supported z/OS Version 2 Release 1.

Changes made in z/OS Version 2 Release 1, as updated December 2013

This document contains information previously presented in z/OS Communications Server: New Function Summary, GC27-3664-00, which supported z/OS Version 2 Release 1.

New information

Chapter 3, "V2R1 new function summary," on page 27 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 23.

Summary of changes for z/OS Version 2 Release 1

For specifics on the enhancements for z/OS Version 2, Release 1, see the following publications:

- z/OS Summary of Message and Interface Changes
- z/OS Introduction and Release Guide
- z/OS Planning for Installation
- z/OS Migration

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 z Systems™ product line consists of the IBM z13 (z13).
- The IBM zEnterprise® System (zEnterprise) product line consists of the IBM zEnterprise EC12 (zEC12), the IBM zEnterprise BC12 (zBC12), the IBM zEnterprise 196 (z196), and the IBM zEnterprise 114 (z114).
- 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), and 890 (z890).
- 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 z13, zEC12, zBC12, z196, z114, z10 EC, z10 BC, z9 EC (formerly z9-109), z9 BC, z990, and z890 servers are also known as z/Architecture® servers. z/OS V2R1 Communications Server runs only in z/Architecture mode on IBM z Systems, IBM zEnterprise, IBM System z10, and the IBM System z9 servers.

Determining which documents to use when migrating

This table helps you determine which documents to use as you migrate.

Table 1. Comparing documents used in migration

Document name	Descriptions
z/OS Planning for Installation	This document helps you prepare to install z/OS by giving you information that 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. **Recommendation:** It is recommended that you read this document. **Use this document as you prepare to install z/OS.**
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 V2R1 Communications Server.

Level 2

This level of encryption is included in the base of z/OS V2R1 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.

Procedure

1. Understand your network topology, including the hardware and software in your network and your network configuration.
2. Understand that z/OS V2R1 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 V2R1 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 V2R1 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.
   a. Evaluate the z/OS V2R1 Communications Server features and enhancements by reading the new function summary topics in this document.
   b. 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 information 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 V2R1 Communications Server, the product is installed in both traditional MVS data sets and in files in the z/OS UNIX file system. For details on changes in the MVS data sets, see "MVS data sets." For details on requirements for hierarchical file system files, see "File system files" on page 7.

MVS data sets

Table 2 lists the distribution library data sets required by z/OS V2R1 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

Table 2. Distribution library data sets (continued)

Data set	Description
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)
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 V2R1 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

Table 3. Target library data sets (continued)

Data set	Description
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
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 V2R1 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)

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

Data set	Description
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
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 V2R1 Communications Server. Table 5 shows the z/OS data sets that contain information for z/OS V2R1 Communications Server, and Table 6 on page 10 shows the z/OS data sets that contain information for both VTAM and NCP.

Enterprise Extender requires IP data set 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.

Tip: The data sets referenced in this section are not necessarily under the SYS1 HLQ. In fact, the entire name for some data sets can be different.

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.

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

Name of data set	Contents	Comments
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.
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.

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

Name of data set	Contents	Comments
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.
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 on page 10 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.
SYS1.SSPLIB	NCP loader utility program	Required; added when NCP is installed. See "SYS1.SSPLIB" on page 20 for information on SYS1.SSPLIB requirements.
	NCP dump utility program	Required; added when NCP is installed. See "SYS1.SSPLIB" on page 20 for information on SYS1.SSPLIB requirements.
	NCP dump bootstrap program	Required; added when NCP is installed. See "SYS1.SSPLIB" on page 20 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 V2R1 Communications Server

This section describes data sets that contain information for z/OS V2R1 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 V2R1 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 are 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:

- 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.

- 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

  Restriction: 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 communications 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:

- Each line in IVTPRM00 must start in column one.
- 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 describes 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 1024 KB to 30720 MB. The default is 100 MB.

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

Restriction: 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.

KB Denotes size in kilobytes

MB Denotes size in megabytes.

bufsize
Specifies the size of the buffers in the pool to be created. Valid pool sizes are 4 KB, 16 KB, 32 KB, 60 KB, and 180 KB. *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

4 KB 1 - 256

16 KB
1 - 256

32 KB
1 - 128

60 KB
1 - 68

180 KB
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: User's Guide.

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 V2R1 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
  ```

Rule: Do not modify any of the foregoing data sets.

Guidelines:

- 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.
- 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.

Using configuration restart data sets

To use the z/OS Communications Server configuration restart facility, define configuration restart Virtual Storage Access Method (VSAM) data sets.

Procedure

To set up data sets for the major nodes that you will be using with configuration restart, perform the following steps. See z/OS Communications Server: SNA Network Implementation Guide for a description of the configuration restart support.

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.

Dynamically configuring data sets for channel-attached devices

You can dynamically configure channel-attached devices in your network.

Procedure

To prepare your system to support dynamic configuration of channel-attached devices, perform the following steps during your installation. See z/OS Communications Server: SNA Network Implementation Guide for a full description of this support.

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.

Defining a 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.

Procedure

To define a NODELST data set, perform the following steps. See z/OS Communications Server: SNA Network Implementation Guide for more information on how NODELST is used.

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.

Results

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 on page 20 shows the correlation between the DD statement for the NCP load module data set and the **NCP BUILD** definition statement.

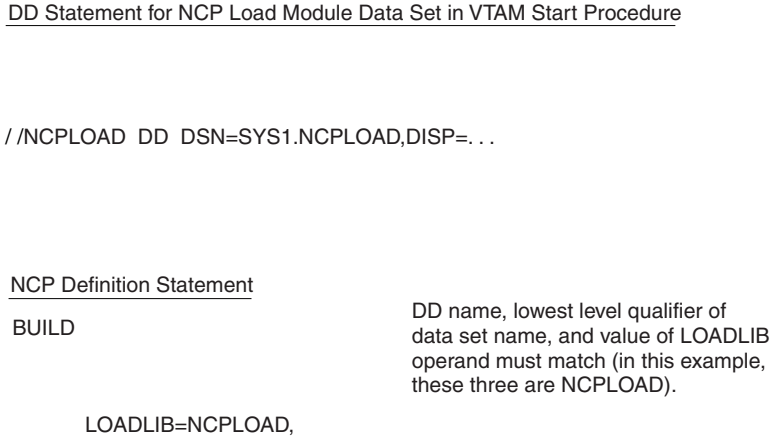

Figure 1. Correlation between DD statement and NCP definition statement

NCP load module data sets must be in an authorized program facility (APF) library. Because 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” 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 V2R1 Communications Server and z/OS V1R13 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 V2R1 Communications Server	
"Enhanced IDS IP fragment attack detection" on page 28	Yes
"Improve auditing of NetAccess rules" on page 28	Yes
"AT-TLS support for TLS v1.2 and related features" on page 28	Yes
"Improved FIPS 140 diagnostics" on page 30	Yes
"Limit defensive filter logging" on page 30	Yes
"QDIO outbound flood prevention" on page 31	No
"TN3270 client-bound data queueing limit" on page 32	Yes
"AT-TLS enablement for DCAS" on page 32	Yes
"Network security enhancements for SNMP" on page 33	Yes
"TLS security enhancements for sendmail" on page 34	Yes
"TLS security enhancements for Policy Agent" on page 35	Yes
"Configuration Assistant performance improvements and enhanced user interface" on page 36	No
"Improve translation of special characters in linemode for TSO/VTAM" on page 36	Yes
"Resolver initialization resiliency" on page 36	Yes
"Enterprise Extender IPv6 address configuration" on page 37	Yes
"Simplified configuration for progressive mode ARB" on page 38	Yes
"Check TCP/IP profile syntax without applying configuration changes" on page 39	Yes
"User control of Ephemeral Port Ranges" on page 40	Yes
"IPv4 INTERFACE statement for HiperSockets and Static VIPAs" on page 41	Yes
"IBM Health Checker for z/OS GATEWAY statement" on page 43	Yes
"CSSMTP mail message date header handling option" on page 44	Yes
"Socket establishment time for Netstat ALL/-A" on page 45	Yes
"Sysplex-wide security associations for IPv6" on page 45	Yes
"HPR PSRETRY Enhancement" on page 46	Yes
"RPCBIND recycle notification" on page 46	Yes
"SNA serviceability enhancements" on page 47	No
"TCP/IP serviceability enhancements" on page 47	No
"API to locate SYSLOGD configuration file" on page 48	Yes
"Real-time application-controlled TCP/IP trace NMI" on page 48	Yes

Table 8. Roadmap to functions (continued)

Functional enhancement	Exploitation actions
"FTP client security user exits" on page 49	Yes
"Simplify FTP transfer of data sets between z/OS systems" on page 50	Yes
"Enable DHCP clients on OSA interfaces" on page 51	Yes
"NMI and SMF enhancements for TCP/IP applications" on page 51	Yes
"QDIO acceleration coexistence with IP filtering" on page 53	Yes
"TCP support for selective acknowledgments" on page 54	Yes
"Shared Memory Communications over Remote Direct Memory Access" on page 55	Yes
"DISPLAY NET, BRFUSE command Enhancement" on page 57	Yes
"Shared Memory Communications over RDMA adapter (RoCE) virtualization" on page 57	Yes
"Connection termination notification for sockets" on page 58	Yes
"IPv6 support for policy-based routing" on page 59	Yes
"Affinity for application-instance DVIPAs" on page 60	Yes
"Enhanced Fast Path socket support" on page 60	No
"Enhanced TCP protocol configuration options and default settings" on page 60	Yes
Enhancements introduced in z/OS V1R13 Communications Server	
"Expanded intrusion detection services" on page 63	Yes
"Network address translation traversal support for IKE version 2" on page 64	Yes
"Sysplex-Wide Security Associations for IKE version 2" on page 65	Yes
"Improved security granularity for VIPARANGE DVIPAs" on page 66	Yes
"FTP support for password phrases" on page 67	Optional
"Removed superuser requirement for Policy Agent and IKE daemon" on page 68	Yes
"Enhanced IPsec support for FIPS 140 cryptographic mode" on page 69	Yes
"Configuration Assistant management of multiple z/OS Communications Server releases" on page 70	Yes
"Configuration Assistant discovery of stack IP addresses" on page 70	Yes
"Configuration Assistant common configuration of multiple stacks" on page 72	Yes
"Configuration Assistant enhancements" on page 73	Yes
"Wildcard support for the PORTRANGE statement" on page 74	Yes
"HiperSockets optimization for intraensemble data networks" on page 74	Yes
"Support for additional VLANs for an OSA-Express QDIO port" on page 75	Yes
"Increased CTRACE and VIT capacity" on page 76	Optional
"OSA-Express4S QDIO IPv6 checksum and segmentation offload" on page 78	Yes
"System resolver autonomic quiescing of unresponsive name servers" on page 79	Yes
"Improved convergence for sysplex distribution routing when joining a sysplex" on page 80	No
"CSSMTP extended retry" on page 80	Yes
"Monitor CSM constrained conditions for sysplex autonomics" on page 81	Optional
"Enhanced FTP support for extended address volumes" on page 82	Yes
"FTP support for large-format data sets" on page 82	Yes
"NMI for retrieving system resolver configuration information" on page 83	Yes

Table 8. Roadmap to functions (continued)

Functional enhancement	Exploitation actions
"Simplified authorization requirements for real-time TCP/IP network monitoring NMI" on page 83	Yes
"Enhancements to the TN3270E server" on page 84	Yes
"CSSMTP enhancements" on page 85	Yes
"Support for bypassing host name lookup in otelnetd" on page 85	Yes
"TCP/IP serviceability enhancements" on page 86	Yes
"Intrusion detection services support for Enterprise Extender" on page 87	Yes
"Enterprise Extender firewall-friendly connectivity test" on page 87	Yes
"HPR packet trace analyzer for Enterprise Extender" on page 88	Yes
"Improved APPN routing resilience" on page 88	No
"Performance improvements for Enterprise Extender traffic" on page 88	Yes

Chapter 3. V2R1 new function summary

This information contains topics about every function or enhancement introduced in z/OS V2R1 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 23 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 V2R1

z/OS V2R1 Communications Server discontinues support of Berkeley Internet Name Domain 9.2.0 (BIND 9.2.0) DNS server function. If you used the z/OS BIND 9.2.0 function as a caching-only name server, use the z/OS resolver DNS caching function to cache DNS responses. If you used the z/OS BIND 9.2.0 function as a primary or secondary authoritative name server, investigate using BIND on Linux for System z® or BIND on an IBM blade in a zBX.

Starting in z/OS V2R1 Communications Server, IBM Configuration Assistant for z/OS Communications Server will no longer be offered as a stand-alone application that runs on the Windows operating system. IBM Configuration Assistant for z/OS Communications Server is available as a fully supported task in the z/OS Management Facility (z/OSMF) product.

See z/OS Migration for detailed information about all the z/OS V2R1 Communications Server support considerations.

Security

The following topics describe enhancements for security:

- "Enhanced IDS IP fragment attack detection" on page 28
- "Improve auditing of NetAccess rules" on page 28
- "AT-TLS support for TLS v1.2 and related features" on page 28
- "Improved FIPS 140 diagnostics" on page 30
- "Limit defensive filter logging" on page 30
- "QDIO outbound flood prevention" on page 31
- "TN3270 client-bound data queueing limit" on page 32
- "AT-TLS enablement for DCAS" on page 32
- "Network security enhancements for SNMP" on page 33
- "TLS security enhancements for sendmail" on page 34
- "TLS security enhancements for Policy Agent" on page 35

Enhanced IDS IP fragment attack detection

z/OS V2R1 Communications Server enhances the Intrusion Detection Services (IDS) IP fragment attack type to detect fragment overlays that change the data in the packet. In addition, the IP fragment attack detection is extended to IPv6 traffic.

Enabling the IDS IP fragment attack detection

To enable the IDS IP fragment attack detection, perform the appropriate task in Table 9.

Table 9. Enhanced IDS IP fragment attack detection

Task	Reference
Enable the IDS IP fragment attack by using one of the following options: • Use the IBM Configuration Assistant for z/OS to enable the Fragment Attack in the IDS requirement map. • Manually configure the IP_Fragment attack in the IDS policy file.	See the following topics: • Intrusion detection services in z/OS Communications Server: IP Configuration Guide • IBM Configuration Assistant for z/OS Communications Server online help • IP_FRAGMENT attack type in z/OS Communications Server: IP Configuration Reference

Improve auditing of NetAccess rules

z/OS V2R1 Communications Server introduces control over the level of caching that is used for network access control checks. You can reduce the level of caching to pass more network access control checks to the System Authorization Facility (SAF). Passing more network access control checks to SAF allows the security server product to provide more meaningful auditing of access control checks.

z/OS V2R1 Communications Server enhances the log string provided to the security server product on each network access control check to include the IP address that the user is attempting to access.

Improving the auditing of NetAccess rules

To improve the auditing of NetAccess rules, perform the appropriate tasks in Table 10.

Table 10. Improve auditing of NetAccess rules

Task	Reference
Set the level of caching that is used for network access control checks by using the CACHEALL, CACHEPERMIT, or CACHESAME keyword on the TCP/IP stack NETACCESS profile statement.	NETACCESS statement in z/OS Communications Server: IP Configuration Reference
Display the level of caching in effect for network access control checks.	DISPLAY TCPIP,,NETSTAT,ACCESS,NETWORK in z/OS Communications Server: IP System Administrator's Commands

AT-TLS support for TLS v1.2 and related features

z/OS V2R1 Communications Server supports Application Transparent TLS (AT-TLS) currency with z/OS System SSL. Support is added for the following functions that are provided by System SSL:

- Renegotiation (RFC 5746) in z/OS V1R12
- Elliptic Curve Cryptography (RFC 4492 and RFC 5480) in z/OS V1R13

- TLSv1.2 (RFC 5246) in z/OS V2R1
- AES GCM Cipher Suites (RFC 5288) in z/OS V2R1
- Suite B Profile (RFC 5430) in z/OS V2R1
- ECC and AES GCM with SHA-256/384 (RFC 5289) in z/OS V2R1

Dependency: Elliptic Curve ciphers and ciphers that use AES-GCM require Integrated Cryptographic Services Facility (ICSF) to be active. If the CSFSERV class is defined, the application user ID must have READ access to certain resources in the CSFSERV class.

Using the AT-TLS support for TLS v1.2 and related features

To use the AT-TLS support for TLS v1.2 and related features, perform the appropriate tasks in Table 11.

Table 11. AT-TLS support for TLS v1.2 and related features

Task	Reference
Enable new AT-TLS policies by using the Configuration Assistant or manual configuration: • If using IBM Configuration Assistant for z/OS Communications Server, migrate your current backing store to V2R1. • Use new AT-TLS statements or parameters as needed in the AT-TLS environment or connection actions.	See the following topics: • IBM Configuration Assistant for z/OS Communications Server online helps • AT-TLS policy statements in z/OS Communications Server: IP Configuration Reference
Optionally, display the policy-based networking information. Use the pasearch command to display AT-TLS policies.	The z/OS UNIX pasearch command in z/OS Communications Server: IP System Administrator's Commands
Before you use Elliptic Curve Cryptography (ECC) ciphers, perform the following steps: 1. Start ICSF. 2. If the CSFSERV class is defined, give the user ID that runs the AT-TLS application READ access to the following resources in that class: • CSF1TRC • CSF1PKV • CSF1PKS • CSF1GKP • CSF1GAV • CSF1DVK • CSF1TRD	Using Cryptographic Features with System SSL in *Cryptographic Services System Secure Sockets Layer programming (SC24-5901-11)*
Before you use AES GCM ciphers, perform the following steps: 1. Start ICSF. 2. If the CSFSERV class is defined, give the user ID that runs the AT-TLS application READ access to the following resources in that class: • CSF1TRC • CSF1SKD • CSF1SKE • CSF1TRD	Using Cryptographic Features with System SSL in *Cryptographic Services System Secure Sockets Layer programming (SC24-5901-11)*

Table 11. AT-TLS support for TLS v1.2 and related features (continued)

Task	Reference
If you intend to use any of the new four character cipher suites, you might need to modify applications: • Use the TTLSi_Neg_Cipher4 field instead of the TTLSi_Neg_Cipher field on the SIOCTTLSCTL ioctl. • Use the Network Management Interface NWMTcpConnType to use the NWMConnTTLSNegCiph4 field instead of the NWMConnTTLSNegCiph field. • Process SMF Type 119 records: – TCP Connection Termination to use the SMF119AP_TTTTLSNC4 field instead of the SMF119AP_TTTTLSNC field – CSSMTP Connection Identification to use the SMF119ML_CN_TLSSNC4 field instead of the SMF119ML_ – CN_TLSSNC field FTP Client Transfer Complete to use the SMF119FT_FCCipher4 field instead of the SMF119FT_FCCipher field – FTP Server Transfer Complete to use the SMF119FT_FSCipher4 field instead of the SMF119FT_FSCipher field – FTP Login Failure to use the SMF119FT_FFCipher4 field instead of the SMF119FT_FFCipher field	Network management interfaces and Application Transparent Transport Layer Security (AT-TLS) in z/OS Communications Server: IP Programmer's Guide and Reference
Use new SNMP MIB object ibmMvsTcpConnectionTtlsNegCipher4 to retrieve the four-byte cipher in use on a TCP connection using AT-TLS.	TCP/IP subagent in z/OS Communications Server: IP System Administrator's Commands

Improved FIPS 140 diagnostics

z/OS V2R1 Communications Server provides enhanced diagnostics for the IKE and NSS daemons and the AT-TLS function when FIPS 140 processing is required.

Integrated Cryptographic Services Facility (ICSF) is required when FIPS 140 is configured for the IKE or NSS daemons or for an AT-TLS group. Starting in V2R1, these daemons and the AT-TLS groups will fail to initialize if ICSF is not active.

Dependency: NSSD, IKED, and AT-TLS Groups in FIPS140 mode require ICSF to be active at startup.

Using improved FIPS 140 diagnostics

To use improved FIPS 140 diagnostics, perform the task in Table 12.

Table 12. Improved FIPS 140 diagnostics

Task	Reference
Start NSSD, IKED or a AT-TLS group in FIPS 140 mode.	z/OS Communications Server: IP Configuration Guide

Limit defensive filter logging

The existing defensive filtering function provides a mechanism to install temporary filters to either deny attack packets or log when a packet would have been denied

if blocking mode was used. In z/OS V2R1 Communications Server, you can now limit the number of defensive filter messages that are written to syslogd for a blocking or simulate mode filter. You can configure a default limit to be used for all defensive filters that are added to a TCP/IP stack. You can also specify a limit when adding an individual defensive filter with the z/OS UNIX ipsec command.

Limiting defensive filter logging

To limit defensive filter logging, perform the appropriate tasks in Table 13.

Table 13. Limit defensive filter logging

Task	Reference
This task is optional. Configure a default log limit in the Defense Manager Daemon (DMD) configuration file. Use the DefaultLogLimit parameter on the DmStackConfig statement.	• Defense Manager daemon in z/OS Communications Server: IP Configuration Reference • Defensive Filtering in z/OS Communications Server: IP Configuration Guide
If a default log limit is not added to the DMD configuration file or if you want to override the value in the DMD configuration file, take the following steps: • Update automation or scripts used to add defensive filters. Add the loglimit parameter to the ipsec -F add invocations. • When manually adding defensive filters, include the loglimit parameter on the ipsec -F add command. • Use the ipsec -F update command with the loglimit parameter to update the log limit for an existing defensive filter.	• The z/OS UNIX ipsec command syntax and The z/OS UNIX ipsec command defensive filter (-F) option in z/OS Communications Server: IP System Administrator's Commands • Defensive Filtering in z/OS Communications Server: IP Configuration Guide
Display log limit information for a defensive filter. Use the z/OS UNIX ipsec command with the -F display option.	See the following topics in z/OS Communications Server: IP System Administrator's Commands: • The z/OS UNIX ipsec command syntax • The z/OS UNIX ipsec command defensive filter (-F) option

QDIO outbound flood prevention

z/OS V2R1 Communications Server relieves CSM storage constraints when processing ICMP Timestamp requests.

Because the z/OS TCP/IP stack replies to these requests, a flood of such requests can cause problems under the right conditions. Such a flood causes the TCP/IP stack to back up because it cannot get the responses out quickly enough, which results in a constrained CSM condition.

If the constrained CSM condition is not relieved, it might cause a stack outage. This behavior might happen with:

- Other ICMP requests that always generate a response (for example, echo requests)
- UDP requests to an application that behaves in a similar manner

QDIO outbound packets will be dropped when CSM storage is constrained and the outbound queues are congested. This support alleviates these problems.

Restriction: This support applies only to data sent out over OSA-Express QDIO and HiperSockets interfaces.

TN3270 client-bound data queueing limit

z/OS V2R1 Communications Server introduces MAXTCPSENDQ, a new parameter in the Telnet profile, to prevent large amounts of storage from being held for data that is destined for an unresponsive Telnet client.

Enabling the TN3270 client-bound data queueing limit

To enable the TN3270 client-bound data queueing limit, perform the task in Table 14.

Table 14. TN3270 client-bound data queueing limit

Task/Procedure	Reference
Limit the queueing of data that is destined for an unresponsive Telnet client by specifying the MAXTCPSENDQ parameter in the Telnet profile.	MAXTCPSENDQ statement in z/OS Communications Server: IP Configuration Reference

AT-TLS enablement for DCAS

With APAR PM96898 installed, z/OS V2R1 Communications Server enhances the Digital Certificate Access Server (DCAS) to use Application Transparent Transport Layer Security (AT-TLS). To use TLSv1.2 to secure the connection, you must define AT-TLS policies for the DCAS.

Migrate to AT-TLS to allow the DCAS to use the latest support for SSL/TLS. Configuring TLS/SSL by using the DCAS configuration file is supported, but such support is deprecated and will no longer be enhanced.

Dependency: The Policy Agent must be active.

Using AT-TLS enablement for DCAS

To use this DCAS enhancement, perform the appropriate tasks in Table 15.

Table 15. AT-TLS enablement for DCAS

Task/Procedure	Reference
Enable Transparent Transport Layer Security (TTLS) in the TCP/IP stack by specifying the **TTLS** parameter on the **TCPCONFIG** statement in the TCPIP profile.	• Application Transparent Transport Layer Security data protection in z/OS Communications Server: IP Configuration Guide • TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Set up authorization for the **pasearch** command if the command is not issued from a superuser. To set authorization for the **pasearch** command, create a SERVAUTH profile of `EZB.PAGENT.sysname.TcpImage.ptype`. The `ptype` value can be set to TTLS or a wildcard value.	• Steps for configuring the Policy Agent in z/OS Communications Server: IP Configuration Guide • z/OS Security Server RACF Security Administrator's Guide

Table 15. AT-TLS enablement for DCAS (continued)

Task/Procedure	Reference
Enable AT-TLS configuration for the Policy Agent by specifying **CommonTTLSConfig**, **TLSConfig**, or both statements in the Policy configuration file for each stack.	• Policy-based networking and Application Transparent Transport Layer Security data protection in z/OS Communications Server: IP Configuration Guide • CommonTTLSConfig statement and TTLSConfig statement in z/OS Communications Server: IP Configuration Reference
Define the AT-TLS policies by specifying the policies in the configuration files that are identified with the **CommonTTLSConfig** and **TTLSConfig** statements.	Specify the AT-TLS policies in the configuration files that are identified with the **CommonTTLSConfig** and **TTLSConfig** statements. Use one of the following methods to create the AT-TLS Policy Agent configuration files: • Use the IBM Configuration Assistant for z/OS Communications Server. Through a series of wizards and online help panels, you can use a GUI to produce the Policy Agent configuration files for any number of TCP/IP stacks. Using the GUI can reduce the amount of time that is required to produce configurations and reduce chances of configuration errors. • Code the required statements into a z/OS UNIX file or MVS data set.
Display policy-based networking information by using the z/OS UNIX System Services (USS) **pasearch** command to query information from the z/OS UNIX Policy Agent. The command is issued from the USS shell.	Displaying policy-based networking information in z/OS Communications Server: IP System Administrator's Commands
Enable AT-TLS in the DCAS configuration file by setting **TLSMECHANISM** to ATTLS.	Customizing DCAS for TLS/SSL in z/OS Communications Server: IP Configuration Guide

Network security enhancements for SNMP

With APAR PM96901 installed, z/OS V2R1 Communications Server enhances the SNMP Agent, the z/OS UNIX **snmp** command, and the SNMP manager API to support the Advanced Encryption Standard (AES) 128-bit cipher algorithm as an SNMPv3 privacy protocol for encryption. The AES 128-bit cipher algorithm is a stronger encryption protocol than the current Data Encryption Standard (DES) 56-bit algorithm. AES is a symmetric cipher algorithm that the National Institute of Standards (NIST) selects to replace DES. RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model (USM)*, specifies that Cipher Feedback Mode (CFB) mode is to be used with AES encryption. See Appendix A, "Related protocol specifications," on page 91 for information about accessing RFCs.

Dependency: To use AES 128-bit encryption, the z/OS Integrated Cryptographic Services Facility (ICSF) must be configured and started.

Using network security enhancements for SNMP

To use this SNMP enhancement, perform the appropriate tasks in Table 16.

Table 16. Network security enhancements for SNMP

Task/Procedure	Reference
Configure and start the z/OS Integrated Cryptographic Services Facility (ICSF).	For detailed information about configuring ICSF, see z/OS Cryptographic Services ICSF Administrator's Guide.
For the SNMP Agent, configure an SNMPv3 user to use AES 128-bit encryption by specifying a USM_USER entry with the **privProto** field set to AESCFB128.	For detailed information about the **privProto** parameter, see the following references: • Overview of SNMP security models in z/OS Communications Server: IP Configuration Guide • Coding the SNMPD.CONF entries in z/OS Communications Server: IP Configuration Reference
For the z/OS UNIX **snmp** command, configure an SNMPv3 user to use AES 128-bit encryption by specifying a configuration statement with the **privProto** field set to AESCFB128.	For detailed information about the **privProto** parameter, see the following references: • Overview of SNMP security models in z/OS Communications Server: IP Configuration Guide • Coding the SNMPD.CONF entries in z/OS Communications Server: IP Configuration Reference
For the SNMP Manager API, configure an SNMPv3 user to use AES 128-bit encryption by specifying a configuration statement with the **privProto** field set to AESCFB128.	SNMP manager API configuration file in z/OS Communications Server: IP Programmer's Guide and Reference

TLS security enhancements for sendmail

With APAR PM96896 installed, z/OS V2R1 Communications Server enables z/OS UNIX sendmail to support TLSv1.1 and TLSv1.2 with a new set of TLSv1.2 2-byte specific ciphers.

Using TLS security enhancements for sendmail

To enable TLSv1.2 with 2-byte ciphers, perform the task in Table 17.

Table 17. TLS security enhancements for sendmail

Task/Procedure	Reference
If System SSL needs to access ICSF for new TLSv1.2 ciphers, ICSF must be started before starting sendmail.	z/OS Cryptographic Services System SSL Programming for information about using hardware Cryptographic Features with System SSL
In the sendmail z/OS specific configuration file (/etc/mail/zOS.cf), update the CipherLevel to use new 2-byte ciphers available with TLSv1.2.	The CipherLevel statement in Creating the z/OS-specific file in z/OS Communications Server: IP Configuration Guide

TLS security enhancements for Policy Agent

With APAR PM96891 installed, z/OS V2R1 Communications Server enables centralized Policy Agent to support TLSv1.1 and TLSv1.2 with a new set of TLSv1.2 2-byte specific ciphers. In addition, the import services between the Policy Agent and IBM Configuration Assistant for z/OS Communications Server allow user-defined AT-TLS policies to create a secure SSL connection.

Using TLS security enhancements for Policy Agent

To update SSL/TLS support in the centralized policy agent and import services, perform the appropriate tasks in Table 18.

Table 18. TLS security enhancements for Policy Agent

Task/Procedure	Reference
If System SSL needs to access ICSF for new TLSv1.2 ciphers, ICSF must be started before starting policy agent.	z/OS Cryptographic Services System SSL Programming for information about using hardware Cryptographic Features with System SSL
In the Policy Agent configuration file (/etc/pagent.conf), you can update ServerConnection/ServerSSLV3CipherSuites to use the TLSv1.1 or TLSv1.2 new 2-byte ciphers for centralized policy agent support.	ServerSSLV3CipherSuites in ServerConnection under Policy Agent general configuration file statements in z/OS Communications Server: IP Configuration Reference
In the Policy Agent configuration file (/etc/pagent.conf), you can set ServicesConnection to Security Basic and use a default unsecure connection, or you can define AT-TLS policies to protect this import services connection with SSL/TLS.	Security Basic in ServicesConnection under Policy Agent general configuration file statements in z/OS Communications Server: IP Configuration Reference

Simplification

The following topics describe enhancements for simplification:

- "Configuration Assistant performance improvements and enhanced user interface" on page 36
- "Improve translation of special characters in linemode for TSO/VTAM" on page 36
- "Resolver initialization resiliency" on page 36
- "Enterprise Extender IPv6 address configuration" on page 37
- "Simplified configuration for progressive mode ARB" on page 38
- "Check TCP/IP profile syntax without applying configuration changes" on page 39
- "User control of Ephemeral Port Ranges" on page 40
- "IPv4 INTERFACE statement for HiperSockets and Static VIPAs" on page 41
- "IBM Health Checker for z/OS GATEWAY statement" on page 43
- "CSSMTP mail message date header handling option" on page 44

Configuration Assistant performance improvements and enhanced user interface

z/OS V2R1 Communications Server enhances Configuration Assistant to support a new Web 2.0 design model on z/OSMF. This provides the following improvements to performance and user experience:

- A redesigned user interface that provides an integrated experience with other z/OSMF applications
- Improved performance that reduces the server-side processing on z/OS

Improve translation of special characters in linemode for TSO/VTAM

z/OS V2R1 Communications Server enhances TSO/VTAM to translate Extended English characters for the TPUT macro instruction with the EDIT parameter. For more information about the Extended English translation, see *D/T3174 Character Set Reference*.

This function provides the following options for the TPUT EDIT translation for terminals that support the Extended English character set:

- Base English translation
- No translation
- Extended English translation

In previous releases, TSO/VTAM translated the Extended English characters of the TPUT EDIT to colons. The colons were then sent to terminals that supported the Extended English character set (Coded Graphic Set Global Identifier (CGCSGID) of X'02B90025').

Improving translation of special characters in linemode for TSO/VTAM

To improve translation of special characters in linemode for TSO/VTAM, perform the task in Table 19.

Table 19. Improve translation of special characters in linemode for TSO/VTAM

Task	Reference
Choose basic English translation, Extended English translation, or no translation for TPUT EDIT to terminals that support the Extended English character set by specifying the parameter ENGTRANS with the appropriate value in the system parmlib member TSOKEY00.	ENGTRANS parameter in TSOKEY00 in z/OS MVS Initialization and Tuning Reference.

Resolver initialization resiliency

z/OS V2R1 Communications Server provides enhancements to the system resolver to start regardless of the following conditions:

- The resolver detects one or more errors with the statements in the resolver setup file.
- The resolver setup file does not exist or cannot be accessed by the resolver.
- One or more files that are specified as values on the resolver setup statements, such as GLOBALTCPIPDATA, do not exist or cannot be accessed by the resolver.

The resiliency of the resolver initialization allows your TCP/IP stacks and other applications that are dependent on resolver processing to continue their initialization despite any resolver setup file errors.

Detecting configuration errors during resolver initialization

To determine whether the system resolver detected errors in the resolver setup file during resolver initialization, perform the appropriate tasks in Table 20.

Table 20. Resolver initialization resiliency

Task	Reference
Create automation to monitor whether the resolver started with configuration errors. This task is optional.	Customizing the Resolver in z/OS Communications Server: IP Configuration Guide
Detect that the resolver started with configuration errors by using one of the following approaches: • Monitor the operator console for message EZD2038I. • Issue the MODIFY RESOLVER,DISPLAY command after system initialization and check for message EZD2039I. If necessary, alert systems programmers to take corrective actions.	Customizing the Resolver in z/OS Communications Server: IP Configuration Guide

Enterprise Extender IPv6 address configuration

z/OS V2R1 Communications Server enhances your ability to configure your IPv6 EE connections by allowing you to specify an IPv6 address instead of a hostname. You can specify IPADDR as any of the following items:

- A VTAM start option
- A parameter on the GROUP statement in an XCA major node
- A parameter on the PATH statement in a switched major node

Requirements:

If you are enabling the new IPv6 IPADDR on a GROUP statement in an XCA major node that defines a connection network on z/OS V2R1 Communications Server, you must apply the PTFs for APAR OA38234 on previous releases of z/OS Communications Server. The PTFs for APAR OA38234 are required to allow a previous release to activate or select an HPR pipe over EE to the z/OS V2R1 Communications Server host using an IPv6 IPADDR for a connection network.

Table 21 indicates the PTFs for APAR OA38234 that are required to make the supported releases compatible with V2R1.

Table 21. PTFs for APAR OA38234

z/OS Communications Server version	PTF for APAR OA38234
V1R12	UA65031
V1R13	UA65032

For distributed Communications Servers or other HPR products to use an HPR pipe over EE to the z/OS V2R1 Communications Server host using an IPv6 IPADDR for a connection network, those products must implement the logic that is needed to support receiving an IPv6 address in the RSCV for an HPR pipe using a connection network. If the destination HPR platform does not support receiving an IPv6 address in the RSCV, the HPR pipe activation or selection fails.

The IPv6 address in the RSCV support is made available in the following product:

Communications Server for Data Center Deployment v7

Configuring an IPv6 address for your EE connections

To configure an IPv6 address for your EE connections, perform the appropriate tasks in Table 22.

Table 22. Enterprise Extender IPv6 address configuration

Task	Reference
Specify an IPv6 address for the IPADDR start option or for the IPADDR operand on the XCA GROUP statement or the Switched EE PATH statement.	See the following topics in z/OS Communications Server: SNA Resource Definition Reference: • IPADDR start option • XCA major node operand IPADDR • Switched major node operand IPADDR or MODIFY VTAMOPTS command in z/OS Communications Server: SNA Operation.
Display the IPADDR start option. Issue the DISPLAY NET,VTAMOPTS,OPTION=IPADDR or the DISPLAY NET,VTAMOPTS command.	DISPLAY VTAMOPTS command in z/OS Communications Server: SNA Operation
Display the IPADDR on the XCA GROUP. Issue the DISPLAY NET,ID=group_name command.	DISPLAY ID command in z/OS Communications Server: SNA Operation
Display the IPADDR on the Switched EE PATH. Issue the DISPLAY NET,PATHS,ID=pu_name command.	DISPLAY PATHS command in z/OS Communications Server: SNA Operation

Simplified configuration for progressive mode ARB

z/OS V2R1 Communications Server simplifies the configuration of the progressive-mode adaptive rate-based (ARB) flow control algorithm on predefined EE Physical Units (PUs). This flow control algorithm improves the performance in virtualized or CPU-constrained environments. You can configure HPREEARB on the GROUP definition statement in the switched major node for predefined EE (Enterprise Extender) connections. As usual, you can also specify the HPREEARB parameter on the following items:

- The PU definition statement in the switched or model (DYNTYPE=EE) major nodes
- The connection network GROUP definition statements in the EE XCA major node

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

Implementing the progressive-mode ARB flow control algorithm for predefined EE PUs

To implement the progressive-mode ARB flow control algorithm for predefined EE PUs, perform the appropriate tasks in Table 23 on page 39.

Table 23. Simplified configuration for progressive mode ARB

Task	Reference
Designate that progressive-mode ARB is to be used for a predefined EE connection by specifying HPREEARB=PROGRESS on the GROUP or PU definition statement in the switched major node.	Switched major node operand HPREEARB in z/OS Communications Server: SNA Resource Definition Reference
Designate that progressive-mode ARB is not to be used for a predefined EE connection by specifying HPREEARB=HPRARB on the GROUP or PU definition statement in the switched major node.	Switched major node operand HPREEARB in z/OS Communications Server: SNA Resource Definition Reference
Determine which ARB mode is being used for a specific HPR pipe by performing the following steps: 1. Issue the DISPLAY ID=rtp_pu,HPRDIAG=YES command. 2. Locate the ARB information in the HPRDIAG output. You can know the status by checking the messages: • If message IST1697I is present, the responsive-mode ARB algorithm is being used. • If message IST2267I is present, the progressive-mode ARB algorithm is being used. • If message IST2395I is present, the base-mode ARB algorithm is being used.	See the following topics: • DISPLAY ID command in z/OS Communications Server: SNA Operation • IST1697I, IST2267I, or IST2395I message in z/OS Communications Server: SNA Messages

Check TCP/IP profile syntax without applying configuration changes

z/OS V2R1 Communications Server improves the availability of TCP/IP by providing a method to check the syntax of TCPIP profile statements in an initial profile or in the profile data set that is specified on a VARY TCPIP,,OBEYFILE command without activating the profile.

With the VARY TCPIP,,SYNTAXCHECK command, you can check the syntax of configuration statements in profile data sets before using the statements to configure TCP/IP.

You do not need to issue the command on the system that will apply the profile; you can check the profile on any system that supports the VARY TCPIP,,SYNTAXCHECK command. For example, you can specify a TCP/IP stack on this command that is configured to support only IPv4 to check a profile that contains IPv6 profile statements.

Restriction: The VARY TCPIP,,SYNTAXCHECK command makes no attempt to update the active configuration; therefore, it does not detect and report conflicts with the active configuration.

Dependencies:

- TCP/IP must be active before you issue this command.
- For consistent syntax checking, you must issue the VARY TCPIP,,SYNTAXCHECK command against a stack that is at the same z/OS release level as the stack that activates the profile.
- If your profile contains MVS system symbols, you must issue the VARY TCPIP,,SYNTAXCHECK command against the same stack that activates the profile to ensure consistent resolution of the MVS system symbols

Checking the TCP/IP profile syntax without applying configuration changes

To check the TCP/IP profile syntax without applying configuration changes, perform the appropriate tasks in Table 24.

Table 24. Check TCP/IP profile syntax without applying configuration changes

Task	Reference
Control which users have access to the VARY TCPIP,,SYNTAXCHECK command.	VARY TCPIP,,SYNTAXCHECK in z/OS Communications Server: IP System Administrator's Commands
Create or update a data set that contains profile statements.	TCP/IP profile (PROFILE.TCPIP) and configuration statements in z/OS Communications Server: IP Configuration Reference
Issue the VARY TCPIP,,SYNTAXCHECK command to check the syntax of statements in the profile that you have created or updated.	VARY TCPIP,,SYNTAXCHECK in z/OS Communications Server: IP System Administrator's Commands

User control of Ephemeral Port Ranges

z/OS V2R1 Communications Server provides new TCP/IP profile configuration options that allow you to specify the ephemeral port range for use by TCP sockets, UDP sockets, or both. Previously, ephemeral ports were assigned from the range 1024 - 65535. To facilitate port controls on firewalls, you can specify a subset of the 1024 - 65535 range for use as ephemeral ports.

Restriction: You cannot expand the range of ephemeral ports to ports beyond the existing 1024 - 65535 range.

Specifying an ephemeral port range

To specify an ephemeral port range for use by TCP or UDP sockets, perform the appropriate tasks in Table 25.

Table 25. User control of Ephemeral Port Ranges

Task	Reference
Understand the interactions of the methods of TCP and UDP socket port restriction.	See the parameters INADDRANYPORT and INADDRANYCOUNT of BPXPRMxx in z/OS MVS Initialization and Tuning Reference See the following topics in z/OS Communications Server: IP Configuration Reference: • GLOBALCONFIG statement • PORT statement • PORTRANGE statement • TCPCONFIG statement • UDPCONFIG statement • VIPADYNAMIC – VIPADISTRIBUTE statement
Restrict the range of ports to be used as ephemeral ports for TCP sockets.	TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Restrict the range of ports to be used as ephemeral ports for UDP sockets.	UDPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display the ranges of ports to be used as ephemeral ports for TCP and UDP sockets.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands

Table 25. User control of Ephemeral Port Ranges (continued)

Task	Reference
Determine whether the ranges of ports to be used as ephemeral ports for TCP and UDP sockets are sufficient for your application needs.	Netstat STATS/-S report in z/OS Communications Server: IP System Administrator's Commands

IPv4 INTERFACE statement for HiperSockets and Static VIPAs

In z/OS V2R1 Communications Server, you can use the INTERFACE statement in the TCP/IP profile to configure IPv4 interfaces for HiperSockets and static VIPAs. This enhancement has the following benefits:

- Simplifies IPv4 configuration for HiperSockets and static VIPA by supporting an INTERFACE statement to replace the DEVICE/LINK/HOME statements.
- Provides a more straightforward way of configuring the source VIPA for IPv4 HiperSockets interfaces.
- Allows you to configure multiple VLANs from the same TCP/IP stack for a single HiperSockets CHPID for both IPv4 and IPv6.

Restrictions:

- z/OS CS supports a maximum of eight VLANs per HiperSockets CHPID per z/OS image per IP version.
- To designate a static VIPA as the source VIPA for an IPv4 interface that is configured using DEVICE and LINK statements, you must configure that static VIPA using DEVICE and LINK statements.

Using the IPv4 INTERFACE statement for HiperSockets and Static VIPAs

To use the IPv4 INTERFACE statement for HiperSockets and Static VIPAs, perform the appropriate tasks in Table 26.

Table 26. IPv4 INTERFACE statement for HiperSockets and Static VIPAs

Task	Reference
To use the INTERFACE statement for an IPv4 HiperSockets interface, take the following steps: 1. Configure the INTERFACE statement for IPAQIDIO in the TCPIP profile. 2. Optionally, specify a source VIPA for this interface by using the SOURCEVIPAINTERFACE parameter. 3. Activate the interface by using the START statement or VARY TCPIP,,START command, and by specifying the interface name.	INTERFACE statement – IPAQIDIO in z/OS Communications Server: IP Configuration Reference

Table 26. IPv4 INTERFACE statement for HiperSockets and Static VIPAs (continued)

Task	Reference
To convert existing IPv4 HiperSockets definitions to use the INTERFACE statement, take the following steps: 1. Replace DEVICE and LINK statements for IPAQIDIO with the new IPv4 INTERFACE statement for IPAQIDIO. 2. Remove the HOME entry and any BSDROUTINGPARMS entry for the interface. 3. If you are currently using the order of your HOME list to designate the source VIPA to be associated with this interface, specify the name of the appropriate static VIPA on the SOURCEVIPAINTERFACE parameter of the IPAQIDIO INTERFACE statement. 4. If you are currently configuring any static routes over this interface using the GATEWAY statement, convert the GATEWAY statement to a BEGINROUTES block.	• Steps for converting from IPv4 IPAQIDIO DEVICE, LINK, and HOME definitions to the IPv4 IPAQIDIO INTERFACE statement in z/OS Communications Server: IP Configuration Guide • INTERFACE statements - IPAQIDIO and BEGINROUTES in z/OS Communications Server: IP Configuration Reference
To use the INTERFACE statements to define an IPv4 static VIPA interface, configure the IPv4 INTERFACE statement for VIRTUAL in the TCPIP profile.	INTERFACE statement - VIRTUAL in z/OS Communications Server: IP Configuration Reference
To convert existing IPv4 static VIPA definitions to use the INTERFACE statement, take the following steps: • Replace the DEVICE and LINK statements for VIRTUAL with the new IPv4 INTERFACE statement for VIRTUAL. • Remove the HOME entry and any BSDROUTINGPARMS entry for the interface.	• Steps for converting from IPv4 VIRTUAL DEVICE, LINK, and HOME definitions to the IPv4 VIRTUAL INTERFACE statement in z/OS Communications Server: IP Configuration Guide • INTERFACE statement - VIRTUAL in z/OS Communications Server: IP Configuration Reference
To configure multiple VLANs for a HiperSockets CHPID, take the following steps: • For IPv4, use the new IPv4 INTERFACE statement for IPAQIDIO. For IPv6, use the existing IPv6 INTERFACE statement for IPAQIDIO6. For each interface, specify the VLAN ID using the VLANID parameter. • For each IPv4 interface for this HiperSockets CHPID, configure a unique subnet using the subnet mask specification on the IPADDR parameter.	See the following topics in z/OS Communications Server: IP Configuration Reference: • INTERFACE statement – IPAQIDIO • INTERFACE statement – IPAQIDIO6
To configure a source VIPA for IPv4 dynamic XCF interfaces, configure the SOURCEVIPAINTERFACE parameter on the IPCONFIG DYNAMICXCF statement in the TCPIP profile.	IPCONFIG statement in z/OS Communications Server: IP Configuration Reference
To display information about IPv4 HiperSockets and static VIPA interfaces that were configured using the INTERFACE statement, issue the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d in z/OS Communications Server: IP System Administrator's Commands
To limit a Netstat display to only show the interfaces that are associated with a specific HiperSockets TRLE, specify the TRLE name on the INTFName/-K filter when using either the Netstat DEvlinks/-d or HOme/-h command.	See the following topics in z/OS Communications Server: IP System Administrator's Commands: • Netstat DEvlinks/-d • Netstat HOme/-h

Table 26. IPv4 INTERFACE statement for HiperSockets and Static VIPAs (continued)

Task	Reference
To display information about the dynamic HiperSockets TRLEs and the datapath devices, issue the D NET,ID=trle, or D NET,TRL,TRLE= command.	See the following topics in z/OS Communications Server: SNA Operation: • DISPLAY ID command • DISPLAY TRL command

IBM Health Checker for z/OS GATEWAY statement

z/OS V2R1 Communications Server provides a new z/OS Health Checker for z/OS migration health check to help determine whether you are using the GATEWAY configuration statement in your TCP/IP profile. Support for the GATEWAY statement will be removed in a future z/OS release. If the GATEWAY statement is processed, a warning message EZZ0717I is issued.

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 migration check support

To use the IBM Health Checker for z/OS migration check support, perform the task in Table 27.

Table 27. IBM Health Checker for z/OS migration check support

Task	Reference
To use the IBM Health Checker for z/OS migration check support, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R1_CS_GATEWAY migration check. 3. 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

IBM Health Checker for z/OS legacy device types

z/OS V2R1 Communications Server, with TCP/IP APAR PI12981 and SNA APAR OA44671, provides a new migration health check to use with the IBM Health Checker for z/OS function. The new migration health check determines whether you are using legacy device type configuration statements in your TCP/IP profile.

Support for the DEVICE and LINK profile statements for the following TCP/IP legacy device types will be eliminated in a future release of IBM z/OS Communications Server:

- ATM
- CDLC
- CLAW
- HYPERchannel
- SNALINK (LU0 and LU6.2)
- X.25

Because support will be eliminated for the ATM device type, the following associated TCP/IP profile statements will no longer be supported:

- ATMARPSV
- ATMLIS
- ATMPVC

When the TCP/IP stack processes a legacy device type profile statement, it issues message EZZ0717I. See this message, and the associated profile processing messages, for information on the profile data set that contains the statements.

Dependency: You must install TCP/IP APAR PI12981 and SNA APAR OA44671 and start the IBM Health Checker for z/OS to use the new migration health check.

IBM Health Checker for z/OS legacy device types

To use the IBM Health Checker for z/OS migration health check support, complete the task in Table 28.

Table 28. IBM Health Checker for z/OS legacy device types

Task	Reference
To use the new migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R1_CS_LEGACYDEVICE migration health check. 3. Review health check output for potential migration actions. Use the TCP/IP EZZ0717I message to locate the profile data sets containing the legacy device type statements.	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

CSSMTP mail message date header handling option

In z/OS V2R1 Communications Server, you can configure the Communications Server Simple Mail Transfer Protocol (CSSMTP) to not add the Date header to the mail message when one was not explicitly specified.

Using the CSSMTP mail message date header handling option

To use the CSSMTP mail message date header handling option, perform the task in Table 29.

Table 29. CSSMTP mail message Date header handling option

Task	Reference
Specify Date No on the CSSMTP configuration Header statement to not add Date header to the mail message if one was not explicitly specified.	CSSMTP Header statement in z/OS Communications Server: IP Configuration Reference

Availability

The following topics describe enhancements for availability:

- "Socket establishment time for Netstat ALL/-A" on page 45
- "Sysplex-wide security associations for IPv6" on page 45
- "HPR PSRETRY Enhancement" on page 46

- "RPCBIND recycle notification" on page 46
- "SNA serviceability enhancements" on page 47
- "TCP/IP serviceability enhancements" on page 47

Socket establishment time for Netstat ALL/-A

z/OS V2R1 Communications Server enhances the Netstat ALL/-A report output by adding start date and time information for TCP connections and UDP endpoints. For TCP connections, the start date and time indicate the occurrence of the following socket functions for the TCP socket:

- Bind
- Listen
- Connection establishment

For UDP endpoints, the start date and time indicate the occurrence of the bind socket function for the UDP socket. The start time information is useful for performance or problem analysis.

Obtaining the start time of the connection

To obtain the start time of a connection, perform the task in Table 30.

Table 30. Obtain the start time of the connection

Task	Reference
Display the following information for TCP connections and UDP endpoints: • UDP bind time • TCP bind time • TCP listen time • TCP connection establishment time	Netstat ALL/-A report in z/OS Communications Server: IP System Administrator's Commands

Sysplex-wide security associations for IPv6

z/OS V2R1 Communications Server provides the support for IPv6 in a sysplex-wide security association (SWSA) environment. Sysplex distribution provides better workload balancing because it performs the following actions:

- Optimally routes new work to the target system and the server application, based on WLM advice
- Increases the availability of workloads by routing traffic around failed components
- Increases flexibility by adding additional workload in a nondisruptive manner

SWSA adds to the sysplex function, distributing the IPSec cryptographic processing for an IPSec security association (SA) among systems in a sysplex environment. SWSA also allows workloads with IPSec-protected traffic to use the dynamic virtual IP address (DVIPA) takeover function. You can associate IPSec-protected workloads with DVIPAs that can be recovered by other systems in the case of a failure or planned takeover. IPSec SAs are automatically reactivated on another system in the sysplex when a DVIPA takeover occurs.

Restrictions:

- All target systems must be at V2R1 or later to distribute workload for IPv6 traffic that is protected by an SA.

- The backup TCP/IP stack must be on a system that is V2R1 or later to take over IPSec-protected workloads with IPv6 DVIPAs.

Using the support for IPv6 in a sysplex-wide security association (SWSA) environment

To use the support for IPv6 in a SWSA environment, perform the appropriate tasks in Table 31.

Table 31. Sysplex-wide security associations for IPv6

Task	Reference
Learn about SWSA.	Sysplex-wide security associations and IP security in z/OS Communications Server: IP Configuration Guide
Configure IPCONFIG6 IPSECURITY and IPSEC DVIPSEC in the distributor stack TCP/IP profile to enable IPv6 SWSA.	IPCONFIG6 statement and IPSEC statement in z/OS Communications Server: IP Configuration Reference
Use the ipsec command to display whether SWSA is enabled.	The ipsec command general report concepts in z/OS Communications Server: IP System Administrator's Commands

HPR PSRETRY Enhancement

z/OS V2R1 Communications Server enhances the HPR PSRETRY function with an additional option to enable the immediate path switch of HPR Rapid Transport Protocol (RTP) pipes. With this option, you can set large PSRETRY values and still have the benefit of immediate searches for preferred session paths when a local link is activated or changes status.

Enabling the immediate path switch of HPR RTP pipes

To enable the immediate path switch of HPR RTP pipes when a local link is activated or changed, perform the task in Table 32.

Table 32. HPR PSRETRY Enhancement

Task	Reference
Enable immediate PSRETRY path switch function.	PSRETRY start option in z/OS Communications Server: SNA Resource Definition Reference

RPCBIND recycle notification

The rpcbind server is improved to provide notifications at strategic points in processing and to enable more effective programming. The rpcbind server sends an ENF signal when the server is starting and when it is stopping.

- The rpcbind server sends an ENF signal when it has started and is prepared to accept registrations from RPC applications. If the rpcbind server is stopped and restarted, RPC applications can monitor this ENF signal and register again with the rpcbind server.
- The rpcbind server sends an ENF signal when it is stopped or cancelled. If the rpcbind server is not available to RPC clients, RPC applications can monitor this ENF signal and take action.

Enabling RPCBIND recycle notification

To enable the RPCBIND recycle notification function, perform the task in Table 33.

Table 33. RPCBIND recycle notification

Task	Reference
Add code to your RPC server to monitor the rpcbind server for ENF signal 80 with qualifier ENF80_RPC_EVENT. Use the EZAENF80 mapping to determine whether the rpcbind server is starting or stopping.	• The section about the Communications Server ENF signal description in z/OS MVS Programming: Authorized Assembler Services Guide • ENFREQ — Listen for system events in z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG • Using ENF event code 80 to listen for rpcbind events in z/OS Communications Server: IP Programmer's Guide and Reference

SNA serviceability enhancements

z/OS V2R1 Communications Server provides the following SNA serviceability enhancements:

- The APPN route selection trace has been enhanced to provide additional trace entries to diagnose the selection of incorrect routes through the APPN network for LU-LU sessions and for directed searches that are used to locate resources. These trace entries are not in the VTAM internal trace table, but exist in a separate internal route selection trace table. Activate the APPN route selection trace in a Network Node (NN).
- The Coupling Facility Services (CFS) component traces connection-related events in mini-trace tables. You get these traces in the mini-trace tables even if VTAM Internal Trace is not running with the CFS option. Each structure has one mini-trace table, except for the MNPS structure. No action is needed to collect CFS traces in the mini-trace tables.
- A new CPNAME operand is added to the Display NET,EE command. This allows you to display all of the active Enterprise Extender connections to the specified remote CP name.

TCP/IP serviceability enhancements

z/OS V2R1 Communications Server provides the following TCP/IP serviceability enhancements:

- An additional message for configuration errors encountered during device or interface activation is being provided. This new message provides information that easily identifies the reason for the activation failure.
- The FTP client is enhanced with trace messages to assist with the diagnosis of problems that occur when opening files. In addition to the already existing EZA2564W messages documenting a failure, these trace messages will provide additional information about the root cause of the failure. These new messages can be accessed by activating the FTP client's FSC debug option.
- The following OMPROUTE serviceability enhancements are provided:
  - Historical time tables are added to OMPROUTE and the TCP/IP stack to help IBM Support diagnose OMPROUTE unresponsiveness problems related to the sysplex monitoring function.
  - A new OMPROUTE message, EZZ8174I, provides additional information in cases where communication between OMPROUTE and the TCP/IP stack fails.

– A new OMPROUTE console command that displays the global configuration options is provided.
– The OMPROUTE_OPTIONS environment variable is ignored. The hello_hi functionality previously provided by the OMPROUTE_OPTIONS environment variable is always enabled to optimize processing inbound and outbound OSPF hello packets so that potential adjacency failures with neighbors are minimized.

Application, middleware, and workload enablement

The following topics describe enhancements for application, middleware, and workload enablement:

- "API to locate SYSLOGD configuration file"
- "Real-time application-controlled TCP/IP trace NMI"
- "FTP client security user exits" on page 49
- "Simplify FTP transfer of data sets between z/OS systems" on page 50
- "Enable DHCP clients on OSA interfaces" on page 51
- "NMI and SMF enhancements for TCP/IP applications" on page 51

API to locate SYSLOGD configuration file

z/OS V2R1 Communications Server enhances syslog daemon (syslogd) processing to provide the syslogd configuration file location and related information. The ability to find syslogd information helps other programs that need to use the information that is written to syslogd.

Using the API to locate SYSLOGD configuration file

To use the API to locate SYSLOGD configuration file, perform the task in Table 34.

Table 34. API to locate SYSLOGD configuration file

Task	Reference
Locate the SYSLOGD configuration file from your program.	Syslog daemon name/token pair and ECSA storage mapping in z/OS Communications Server: IP Programmer's Guide and Reference

Real-time application-controlled TCP/IP trace NMI

The real-time application-controlled TCP/IP trace network management interface (NMI) is a callable NMI that provides the following information to network management applications based on filters that are set by the application:

- Real-time packet trace information
- Real-time data trace information

Each application that uses the NMI can set its own filters and options to obtain the required data, and the application can request the trace data at any time.

In contrast, the existing real-time TCP/IP network monitoring NMI provides similar trace data based on the global packet trace and data trace settings for the TCP/IP stack. The application has to wait for a token to retrieve the trace data.

To provide access to this NMI and to the information that the NMI provides, you must define new security product resource profiles in the SERVAUTH class. You

can use the DISPLAY TCPIP,,TRACE command to display information about the applications that are using this NMI and the resources that are currently being used by the NMI.

Restriction: For an application to be able to use the NMI, the new security product resource profiles must be defined and the user ID of the application must be given READ access to the profiles.

Using the real-time application-controlled TCP/IP trace NMI

To use the real-time application-controlled TCP/IP trace NMI, perform the appropriate tasks in Table 35.

Table 35. Real-time application-controlled TCP/IP trace NMI

Task	Reference
Develop or enhance an application to use the real-time application-controlled TCP/IP trace NMI.	Real-time application-controlled TCP/IP trace NMI in z/OS Communications Server: IP Programmer's Guide and Reference
Define the RACF resource profiles and authorize the user IDs of the applications to the profiles.	Real-time application-controlled TCP/IP trace NMI in z/OS Communications Server: IP Programmer's Guide and Reference
Display information about applications that are using the NMI.	DISPLAY TCPIP,,TRACE in z/OS Communications Server: IP System Administrator's Commands

FTP client security user exits

In z/OS V2R1 Communications Server, you can control FTP client commands that are sent to the server or monitor the replies that are received from the server by using the following two client user exits:

- FTP command user exit - EZAFCCMD. Use the EZAFCCMD user exit to inspect an FTP command, modify the arguments of an FTP command, reject an FTP command, or end the FTP client address space before the command is sent to the server.
- FTP reply user exit - EZAFCREP. Use the EZAFCREP user exit to inspect the FTP server reply or to end the FTP client address space after the FTP client receives each line of reply that is received from the server.

Restrictions:

FTP client user exits are not supported when the FTP client is invoked in an environment in which the FTP client cannot be executed as an authorized program or command. For example, FTP client user exits are not supported in the dynamic TSO environment that the IKJTSOEV service builds.

The following restrictions are for FTP command user exit EZAFCCMD:

- Some command arguments you can inspect, but not modify. Some command arguments you can modify, but not inspect. Some command arguments you cannot inspect or modify.
- The user exit cannot reject the QUIT command or end the client when the exit processes the QUIT subcommand.

The following restrictions are for the FTP reply user exit EZAFCREP:

- The user exit cannot end the client when the exit processes the QUIT subcommand.

- The user exit cannot end the client for a reply with the reply code in the range of 100 to 199.

Using the FTP client security user exits

To use the FTP client security user exits, perform the appropriate tasks in Table 36.

Table 36. FTP client security user exits

Task	Reference
Write the EZAFCCMD or EZAFCREP FTP client user exit.	See the following topics: • Configuring the optional FTP User exits in z/OS Communications Server: IP Configuration Guide • FTP client user exits in z/OS Communications Server: IP Configuration Reference
Install the EZAFCCMD or EZAFCREP FTP client user exit.	See the following topics: • Using dynamic exits services in z/OS MVS Programming: Authorized Assembler Services Guide • Dynamic Exits Facility in z/OS MVS Installation Exits
Interpret messages and client error codes resulting from using the EZAFCCMD and EZAFCREP user exits.	See the following topics: • Security issues when using FTP and FTP return codes in z/OS Communications Server: IP User's Guide and Commands • Predefined REXX variables in z/OS Communications Server: IP Programmer's Guide and Reference • EZA1xxxx messages in z/OS Communications Server: IP Messages Volume 1 (EZA)
Use the FTP client trace to debug user exits.	FTP Client: Setup and FTP client security exits in z/OS Communications Server: IP Diagnosis Guide

Simplify FTP transfer of data sets between z/OS systems

z/OS V2R1 Communications Server for z/OS FTP supports getting the attributes of an MVS data set on the z/OS FTP server using the new FTP command XDSS.

z/OS V2R1 Communications Server for z/OS FTP also introduces two new FTP subcommands, MVSPut and MVSGet. The MVSPut subcommand transfers an MVS data set from a z/OS FTP client to a z/OS FTP server without the client user needing to know the attributes of the client data set. Likewise, the MVSGet subcommand transfers an MVS data set from a z/OS FTP server to a z/OS FTP client without the client user needing to know the attributes of the server data set. In both cases FTP extracts the attributes of the source data set, and applies them to the target host FTP configuration before the transfer.

Restrictions:

Only the following data set types are supported:

- z/OS physical sequential data set
- z/OS partitioned data set or library
- z/OS generation data set reference

See z/OS Communications Server: IP User's Guide and Commands for additional restrictions.

Dependency: You must log in to a z/OS V2R1 or later FTP server to use the MVSGet and MVSPut subcommands.

Simplifying FTP transfer of data sets between z/OS systems

To simplify FTP transfer of data sets between z/OS systems, perform the task in Table 37.

Table 37. Simplify FTP transfer of data sets between z/OS systems

Task	Reference
Use FTP to transfer an MVS data set without knowing the details of its allocation.	FTP subcommands in z/OS Communications Server: IP User's Guide and Commands

Enable DHCP clients on OSA interfaces

Before z/OS V2R1 Communications Server, to define and activate an OSA-Express QDIO interface, you needed to specify an IP address on the INTERFACE statement. This action prevented applications from implementing a DHCP client on z/OS. In z/OS V2R1 Communications Server, you can define and activate an OSA-Express QDIO interface without specifying an IP address. Applications that implement a DHCP client, such as IBM Rational® Developer for System z Unit Test feature (RDz-UT), can communicate with DHCP servers to dynamically obtain an IP address.

Restriction: The TEMPIP parameter is supported only on the INTERFACE statement for IPv4 OSA-Express QDIO interfaces.

Enabling DHCP clients on OSA interfaces

To enable the DHCP clients on OSA interfaces, perform the appropriate tasks in Table 38.

Table 38. Enable DHCP clients on OSA interfaces

Task	Reference
Define an interface by using the TEMPIP keyword.	• Interface – IPAQENET OSA-Express QDIO Interfaces statement in z/OS Communications Server: IP Configuration Reference • Using TEMPIP interfaces in z/OS Communications Server: IP Configuration Guide
Display the interface with the Netstat HOme/-h command.	Netstat Home/-h report in z/OS Communications Server: IP System Administrator's Commands

NMI and SMF enhancements for TCP/IP applications

z/OS V2R1 Communications Server adds two new SMF 119 event records:

- The SMF 119, subtype 71 record contains FTP daemon configuration data. This record is created during the FTP daemon initialization when it listens on the listening port successfully for the first time. A new FTP.DATA statement SMFDCFG is added to control whether to write this SMF record to the SMF data set.
- The SMF 119, subtype 24 record provides the TN3270 server initial profile configuration information, as well as information about replacement of the profile caused by VARY TCPIP,Telnet,OBEYFILE processing. This record is written to the MVS SMF data sets.

In z/OS V2R1 Communications Server, you can obtain FTP daemon configuration data by using the following NMIs:

- The TCP/IP callable NMI, EZBNMIFR, by specifying the new request type, GetFTPDaemonConfig.
- The real-time TCP/IP network monitoring NMI, SYSTCPSM. The SMF type 119, subtype 71 record for FTP daemon configuration data is available to this NMI.

In addition, TN3270 server profile configuration data can be obtained through the following NMIs:

- The TCP/IP callable NMI, EZBNMIFR by specifying the new request type, GetTnProfile.
- The real-time TCP/IP network monitoring NMI, SYSTCPSM. The SMF type 119, subytpe 24 record for TN3270 server profile configuration data is available to this NMI.

The new SMF 119 event record is subtype 24 and is written to the MVS SMF data sets. The event record can also be obtained from the real-time TCP/IP network monitoring NMI (SYSTCPSM). The new SMF record provides the initial profile and information about replacement of the profile caused by VARY TCPIP,Telnet,OBEYFILE processing.

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

Using NMI and SMF enhancements for TCP/IP applications

To obtain FTP daemon configuration data, perform the appropriate tasks in Table 39.

Table 39. NMI and SMF enhancements for TCP/IP applications about FTP daemon configuration data

Task	Reference
Obtain FTP daemon configuration data from the TCP/IP Callable NMI by developing or enhancing an application to use the new TCP/IP callable NMI request, GetFTPDaemonConfig.	Network management interfaces in z/OS Communications Server: IP Programmer's Guide and Reference
Interpret return values, return codes, and reason codes that result from calling the TCP/IP callable NMI EZBNMIFR.	Network management interfaces in z/OS Communications Server: IP Programmer's Guide and Reference
Configure SMFDCFG statement in server FTP.DATA to write type 119 SMF record for FTP daemon configuration data into SMF data sets. The statement has no effect on whether the new SMF record is available to the real-time SMF data NMI or not.	File Transfer Protocol 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 71 event records by specifying NETMONITOR SMFSERVICE PROFILE in the PROFILE.TCPIP configuration file.	NETMONITOR statement in z/OS Communications Server: IP Configuration Reference

Table 39. NMI and SMF enhancements for TCP/IP applications about FTP daemon configuration data (continued)

Task	Reference
Enable applications to obtain the SMF 119 subtype 71 event records from the real-time TCP/IP network monitoring NMI (SYSTCPSM) by configuring the user IDs that are associated with 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

To obtain TN3270 server profile configuration data, perform the appropriate tasks in Table 40.

Table 40. NMI and SMF enhancements for TCP/IP applications about TN3270 server profile configuration data

Task	Reference
Configure the creation of the SMF 119 subtype 24 event records that provide TN3270 server profile information by specifying SMFCONFIG in the PROFILE.TELNET 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 24 event records by specifying 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 24 event records from the real-time TCP/IP network monitoring NMI (SYSTCPSM) by configuring the user IDs that are associated with 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 TN3270 server profile information from the TCP/IP Callable NMI by developing or enhancing an application to use the new TCP/IP Callable NMI request, GetTnProfile.	TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer's Guide and Reference

Economics and platform efficiency

The following topics describe enhancements for economics and platform efficiency:

- "QDIO acceleration coexistence with IP filtering"
- "TCP support for selective acknowledgments" on page 54
- "Shared Memory Communications over Remote Direct Memory Access" on page 55
- "Connection termination notification for sockets" on page 58
- "IPv6 support for policy-based routing" on page 59
- "Affinity for application-instance DVIPAs" on page 60
- "Enhanced Fast Path socket support" on page 60
- "Enhanced TCP protocol configuration options and default settings" on page 60

QDIO acceleration coexistence with IP filtering

z/OS V2R1 Communications Server allows the QDIO Accelerator function, which provides accelerated forwarding of packets, to be enabled when IP Security is enabled. In previous releases, QDIO Accelerator could not be enabled if IP Security was enabled.

Restrictions:

- If your IP filter rules and defensive filter rules do not explicitly permit all routed traffic, QDIO Accelerator forwards only Sysplex Distributor traffic. In this case, routed traffic is processed by the forwarding stack.
- If your IP filter rules or defensive filter rules permit all routed traffic but require routed traffic to be logged, QDIO Accelerator forwards only Sysplex Distributor traffic. In this case, routed traffic is processed by the forwarding stack.
- The QDIO Accelerator function is available for IPv4 traffic only.

Allowing QDIO acceleration to coexist with IP filtering

To allow QDIO acceleration to coexist with IP filtering, perform the appropriate tasks in Table 41.

Table 41. QDIO acceleration coexistence with IP filtering

Task	Reference
Enable QDIO Accelerator with IP security.	IPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Understand the restrictions for QDIO Accelerator and IP security, and how to configure your filter rules so that QDIO Accelerator is able to forward routed traffic.	QDIO Accelerator and IP security in z/OS Communications Server: IP Configuration Guide

TCP support for selective acknowledgments

z/OS V2R1 Communications Server provides the following TCP support for selective acknowledgments:

- Generation of TCP selective acknowledgments as defined in RFC 2018
- Exploitation of incoming TCP selective acknowledgments to improve TCP retransmission processing as defined in RFC 3517

A TCP connection might experience poor performance when multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can learn about only a single lost packet per round-trip time. A Selective Acknowledgment (SACK) mechanism, combined with a selective repeat retransmission policy, can help to overcome these limitations. The receiving TCP sends back SACK packets to the sender informing the sender of data that has been received. The sending TCP can then retransmit only the missing data segments.

Using the TCP support for selective acknowledgments

To use the TCP support for selective acknowledgments, perform the appropriate tasks in Table 42.

Table 42. TCP support for selective acknowledgments

Task	Reference
Disable the exchange of selective acknowledgments.	NOSELECTIVEACK configuration option on the TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference

Table 42. TCP support for selective acknowledgments (continued)

Task	Reference
Determine whether the selective acknowledgment function is enabled: • Issue the Netstat CONFIG/-f command. • Update your network management application to use the information that is returned by the GetProfile callable NMI.	• Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands • GetProfile request in z/OS Communications Server: IP Programmer's Guide and Reference
Configure the creation of the SMF 119 subtype 4 event records that provide TCP/IP profile information.	SMFCONFIG statement in z/OS Communications Server: IP Configuration Reference

Shared Memory Communications over Remote Direct Memory Access

z/OS V2R1 Communications Server provides significant performance improvements for TCP protocol workloads on external networks. This solution uses Shared Memory Communications over Remote Direct Memory Access (SMC-R) for TCP connections to remote peers on external networks that also support this function.

Restrictions:

- This function does not support external networks that contain a mix of interfaces, where some interfaces specify a VLAN ID and some interfaces do not specify a VLAN ID.

Incompatibilities: This function does not support 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 requires the IBM zEnterprise EC12 (zEC12) with driver 15, the IBM zEnterprise BC12 (zBC12), or later.
- This function requires at least one IBM 10GbE RoCE Express feature that is configured in the hardware configuration definition (HCD) with a Peripheral Component Interconnect Express (PCIe) function ID (PFID).

Using Shared Memory Communications over Remote Direct Memory Access

To use Shared Memory Communications over Remote Direct Memory Access, perform the appropriate tasks in Table 43.

Table 43. Shared Memory Communications over Remote Direct Memory Access

Task	Reference
If you are using IPv4 QDIO interfaces that are defined with the DEVICE, LINK, and HOME statements, convert those definitions to use the IPAQENET INTERFACE statement.	Steps for converting from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement in z/OS Communications Server: IP Configuration Guide
Configure at least one 10GbE RoCE Express feature in HCD.	*z/OS Hardware Configuration Definition (HCD) Reference Summary*

Table 43. Shared Memory Communications over Remote Direct Memory Access (continued)

Task	Reference
Select a unique physical network (PNet) ID for each of the networks. Configure the appropriate PNet ID in HCD for each OSD CHPID on a network and configure the PNet ID on each 10GbE RoCE Express interface to be used on that network	*z/OS Hardware Configuration Definition (HCD) Reference Summary*
Configure SMCR on the GLOBALCONFIG statement in the TCP/IP profile, and specify the PFID and optionally the port number corresponding to each 10GbE RoCE Express interface.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
For each IPv4 interface to be used for SMC-R, configure a nonzero subnet mask on the INTERFACE statement in the TCP/IP profile and use the same subnet value as the remote peer stack. For each IPv6 interface to be used for SMC-R, ensure that the interface has at least one associated prefix in common with the remote peer stack.	Shared Memory Communications over Remote Direct Memory Access in z/OS Communications Server: IP Configuration Guide
Optionally, restrict SMC-R from being used by certain server applications by coding the NOSMCR option on the PORT or PORTRANGE statement that defines the server port.	PORT statement and PORTRANGE statement in z/OS Communications Server: IP Configuration Reference
Display whether the stack is enabled for SMC-R by issuing the Netstat CONFIG/-f command.	Netstat: CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display the status of the 10GbE RoCE Express feature by issuing the D PCIE command.	D PCIE command in z/OS MVS System Commands
Display information about the dynamic 10GbE RoCE Express TRLEs by issuing the D NET,ID=*trle*, or D NET,TRL,TRLE=*trle* command.	DISPLAY ID command and c in z/OS Communications Server: SNA Operation
Display information about a 10GbE RoCE Express interface by issuing the Netstat DEvlinks/-d command for the 10GbE RoCE Express interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display the PNet ID for an active OSD or 10GbE RoCE Express interface using the Netstat DEvlinks/-d command or by issuing the D NET,ID=*trle* or D NET,TRL,TRLE=*trle* command.	See the following topics: • DISPLAY ID command and DISPLAY TRL command in z/OS Communications Server: SNA Operation • Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display information about the number of sends, receives, and bytes that went over a 10GbE RoCE Express interface by issuing the Netstat DEvlinks/-d command for the 10GbE RoCE Express interface or by using VTAM tuning statistics for the 10GbE RoCE Express interface.	See the following topics: • Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands • MODIFY TNSTAT command in z/OS Communications Server: SNA Operation
Display how many TCP connections are using SMC-R by issuing the Netstat STATS/-S command.	Netstat STATS/-S report in z/OS Communications Server: IP System Administrator's Commands
Display information about which TCP connections are using SMC-R by issuing the Netstat ALL/-A command.	Netstat ALL/-A report in z/OS Communications Server: IP System Administrator's Commands
Display information about storage that is being used by TCP/IP for SMC-R by issuing the D TCPIP,,STOR command.	D TCPIP,,STOR command in z/OS Communications Server: IP System Administrator's Commands

Table 43. Shared Memory Communications over Remote Direct Memory Access (continued)

Task	Reference
Display information about SMC-R link groups and the associated SMC-R links by issuing the Netstat DEvlinks/-d command with the SMC parameter. Use this information to verify the redundancy level of each SMC-R link group.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

DISPLAY NET, BRFUSE command Enhancement

z/OS V2R1 Communications Server can display the amount of 64-bit storage that is allocated by using the D NET,BFRUSE command.

DISPLAY NET, BRFUSE command Enhancement

To display how much 64-bit storage is allocated, complete the task in Table 44.

Table 44. Shared Memory Communications over RDMA Enhancements

Task	Reference
Display the 64-bit storage usage with the D NET,BFRUSE command.	D NET,BFRUSE command in SNA Operation

Shared Memory Communications over RDMA adapter (RoCE) virtualization

This function extends the Shared Memory Communications over Remote Direct Memory Access (SMC-R) function to allow TCP/IP stacks on different LPARs within the same central processor complex (CPC) to share the same physical IBM 10GbE RoCE Express feature.

Restriction:

- Each TCP/IP stack that shares the same physical 10GbE RoCE Express feature must use a unique function ID (FID) and virtual function number (VFN) to represent the feature. Define the FID and VFN values in the Hardware Configuration Definition (HCD).

Dependencies:

- This function requires IBM z13 (z13) or later systems.
- This function requires at least one IBM 10GbE RoCE Express feature configured in the HCD with a FID and a VFN value.
- The PTFs for APARs OA44576 and PI12223 must be applied.

Shared Memory Communications over RDMA adapter (RoCE) virtualization

To exploit the Shared Memory Communications over RDMA Adapter (RoCE) virtualization function, complete the tasks in Table 45 on page 58.

Table 45. Shared Memory Communications over RDMA adapter (RoCE) virtualization

Task	Reference
Configure at least one IBM 10GbE RoCE Express feature in HCD. If you have existing 10GbE RoCE Express definitions, update the definition to include a VFN value. For each unique combination of PCHID and VFN values, configure a unique function ID (FID) value.	*z/OS Hardware Configuration Definition (HCD) Reference Summary*
Configure or update the GLOBALCONFIG SMCR statement in the TCP/IP profile. • If you have existing PFID definitions on the GLOBALCONFIG statement and you changed the FID value in the HCD for the 10GbE RoCE Express feature, update the existing GLOBALCONFIG PFID values to specify the new FID value. • If you define PFID values, choose PFID values that represent physically different 10GbE RoCE Express features to provide full redundancy support.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference Shared Memory Communications over Remote Direct Memory Access in z/OS Communications Server: IP Configuration Guide
Verify the GLOBALCONFIG SMCR settings by issuing the `Netstat CONFIG/-f` command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display the status of the 10GbE RoCE Express feature by issuing the `D PCIE` command.	Displaying PCIE information in z/OS MVS System Commands
Verify that the correct VFN and PNetID values are assigned to the dynamic 10GbE RoCE Express TRLEs by issuing the `D NET,ID=trle`, or `D NET,TRL,TRLE=trle` command.	DISPLAY ID command and DISPLAY TRL command in z/OS Communications Server: SNA Operation
Display information about a 10GbE RoCE Express interface by issuing the `Netstat DEvlinks/-d` command and specifying the 10GbE RoCE Express interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

Connection termination notification for sockets

In z/OS V2R1 Communications Server, an application can issue a synchronous or an asynchronous receive socket API call that completes only when a TCP connection is ended.

This support is available on the recv(), recvfrom(), and recvmsg() functions in the z/OS XL C/C++ Runtime Library. The support is also available on the recv(BPX1RCV, BPX4RCV), recvfrom(BPX1RFM, BPX4RFM), recvmsg(BPX2RMS, BPX4RMS), and asyncio(BPX1AIO, BPX4AIO) assembler callable services.

Restriction: This enhancement is supported for TCP sockets, but not for UDP or RAW sockets.

Receiving notification of the termination of a socket connection

To receive a notification when a socket connection is terminated, perform the task in Table 46 on page 59.

Table 46. Connection termination notification for sockets

Task	Reference
Issue the receive socket call with the flag value MSG_CONNTERM.	• Recv(), recvfrom(), and recvmsg() in z/OS XL C/C++ Runtime Library Reference • Recv(BPX1RCV, BPX4RCV), recvfrom(BPX1RFM, BPX4RFM), and recvmsg(BPX2RMS, BPX4RMS) in z/OS UNIX System Services Programming: Assembler Callable Services Reference • Asyncio(BPX1AIO, BPX4AIO), AioCmd=Aio#Recv, AioCmd=Aio#RecvFrom, and AioCmd=Aio#RecvMsg in z/OS UNIX System Services Programming: Assembler Callable Services Reference

IPv6 support for policy-based routing

With IPv6 policy-based routing, the TCP/IP stack can make IPv6 routing decisions that take into account criteria other than just the destination IP address. The additional criteria can include job name, source port, destination port, protocol type (TCP or UDP), source IP address, NetAccess security zone, and security label.

Restriction: IPv6 policy-based routing applies only to TCP and UDP traffic that originates at the TCP/IP stack. The following two kinds of IPv6 traffic are routed by using the main route table, even when IPv6 policy-based routing is in use.

- IPv6 traffic that uses protocols other than TCP and UDP
- All IPv6 traffic that is being forwarded by the TCP/IP stack

Using IPv6 support for policy-based routing

To use IPv6 support for policy-based routing, perform the appropriate tasks in Table 47.

Table 47. IPv6 policy-based routing

Task	Reference
Enable IPv6 policy-based routing by using the IBM Configuration Assistant for z/OS Communications Server or manual configuration.	• Policy-based routing in z/OS Communications Server: IP Configuration Guide • IBM Configuration Assistant for z/OS Communications Server online help; see the "What's New in V2R1" help information for IPv6 policy-based routing configuration • Policy-based routing policy statements in z/OS Communications Server: IP Configuration Reference
Issue the **pasearch -R** command to display all routing policy rules and actions.	The z/OS UNIX pasearch command: Display policies in z/OS Communications Server: IP System Administrator's Commands
Issue the **pasearch -T** command to display all route tables.	The z/OS UNIX pasearch command: Display policies in z/OS Communications Server: IP System Administrator's Commands
Issue the **Netstat ROUTe/-r PR** command to display the policy-based routing information.	Netstat ROUTe/-r report in z/OS Communications Server: IP System Administrator's Commands
Issue the **Netstat ALL/-A** command to display the names of the routing policy rule and the policy-based routing table that IP routing uses for an application.	Netstat ALL/-A report in z/OS Communications Server: IP System Administrator's Commands

Table 47. IPv6 policy-based routing (continued)

Task	Reference
Issue the **Display TCPIP,,OMProute,RT6TABLE** command or the **MODIFY procname,RT6TABLE** command with the PRtable parameter to display routes in the OMPROUTE IPv6 policy-based routing tables.	• DISPLAY TCPIP,,OMPROUTE in z/OS Communications Server: IP System Administrator's Commands • MODIFY command: OMPROUTE in z/OS Communications Server: IP System Administrator's Commands

Affinity for application-instance DVIPAs

z/OS V2R1 Communications Server provides support to create a VIPARANGE DVIPA with affinity to the address space of the application that created it. In previous releases, the SIOCSVIPA and SIOCSVIPA6 IOCTL functions and the MODDVIPA utility supported the `define` and `delete` options. In z/OS V2R1 Communications Server, a new `define` with `affinity` option is supported. When an application uses the SIOCSVIPA or the SIOCSVIPA6 IOCTL function to create a DVIPA with the address space `affinity` option, connection requests for this DVIPA are routed to a server that runs in the address space of the application. This behavior is beneficial when there are multiple shareport applications listening on the IPv4 inaddr_any or the IPv6-unspecified address. With this new support, the application that created the DVIPA is preferred over other listeners. If no matching listeners are available, normal shareport load balancing is used to select the best available listener.

Enabling affinity for application-instance DVIPAs

To enable the affinity for application-instance DVIPAs function, perform the appropriate tasks in Table 48.

Table 48. Affinity for application-instance DVIPAs

Task	Reference
To create a VIPARANGE DVIPA with affinity using the SIOCSVIPA or SIOCSVIPA6 ioctl, issue the IOCTL command by using the new DVR_DEFINE_AFFINITY option instead of using DVR_DEFINE.	Using the SIOCSVIPA or SIOCSVIPA6 ioctl command in z/OS Communications Server: IP Configuration Guide
To create a VIPARANGE DVIPA with affinity by using the MODDVIPA utility, issue the MODDVIPA command with the new `-a` option instead of using the `-c` option.	Using the MODDVIPA utility in z/OS Communications Server: IP Configuration Guide

Enhanced Fast Path socket support

z/OS V2R1 Communications Server enhances the performance of the following 6 API calls: recv()/send(), recvfrom()/sendto(), and recvmsg()/sendmsg(). This function is automatically enabled; no tasks are necessary.

Enhanced TCP protocol configuration options and default settings

In z/OS V2R1 Communications Server, the TCP configuration options have the following changes:

- New parameters on the TCPCONFIG statement
- Changes to the default values and limits of existing parameters on the TCPCONFIG and SOMAXCONN statements

Enhanced TCP protocol configuration options and default settings

To use enhanced TCP protocol configuration options and default settings, perform the appropriate tasks in Table 49.

Table 49. Enhanced TCP protocol configuration options and default settings

Task	Reference
Specify the number of seconds that a connection remains in TIMEWAIT state.	The TIMEWAITINTERVAL parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify the maximum retransmit interval for TCP connections.	The MAXIMUMRETRANSMITTIME parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify the maximum number of retransmit attempts for TCP connections.	The RETRANSMITATTEMPTS parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify the total amount of time before the initial connection times out.	The CONNECTTIMEOUT parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify the intial retransmission interval for the connect().	The CONNECTINITINTERVAL parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify whether the Nagle algorithm is disabled globally.	The NAGLE/NONAGLE parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify the maximum number of keep alive probes for TCP connections.	The KEEPALIVEPROBES parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify the interval between keep alive probes for TCP connections.	The KEEPALIVEPROBEINTERVAL parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify a FINWAIT2 time out value less than 60 seconds for TCP connections.	The FINWAIT2 parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify a threshold for engaging TCP outbound serialization.	The QUEUEDRTT parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify the threshold for triggering Fast Retransmit, Fast Recovery processing for TCP connections.	The FRRTHRESHOLD parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Specify a maximum send buffer size for TCP connections.	The TCPMAXSENDBUFRSIZE parameter in TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display the values for the new TCPCONFIG parameters.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display the values for the changed TCPCONFIG parameters.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display the changed SOMAXCONN default value.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands

Chapter 4. V1R13 new function summary

This information contains topics about every function or enhancement introduced in z/OS V1R13 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 23 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 V1R13

IBM intends for z/OS V1R13 to be the final release in which the BIND 9.2.0 function will be available. Customers who currently use or plan to use the z/OS BIND 9.2.0 function as a caching-only name server should use the resolver function, which became generally available in z/OS V1R11, to cache DNS responses. Customers who currently use or plan to use the z/OS BIND 9.2.0 function as a primary or secondary authoritative name server should investigate using BIND on Linux for System z or BIND on an IBM blade in a zBX.

See z/OS Migration for detailed information about all the z/OS V1R13 Communications Server support considerations.

Security

The following topics describe enhancements for security:

- "Expanded intrusion detection services"
- "Network address translation traversal support for IKE version 2" on page 64
- "Sysplex-Wide Security Associations for IKE version 2" on page 65
- "Improved security granularity for VIPARANGE DVIPAs" on page 66
- "FTP support for password phrases" on page 67
- "Removed superuser requirement for Policy Agent and IKE daemon" on page 68
- "Enhanced IPsec support for FIPS 140 cryptographic mode" on page 69
- "Intrusion detection services support for Enterprise Extender" on page 87

Expanded intrusion detection services

z/OS V1R13 Communications Server provides enhancements to intrusion detection services (IDS) in the following areas:

- IDS controls are available to monitor the TCP send, receive, and out-of-order queues for excessive or old data. A new IDS attack type provides the following controls:
  - A configurable threshold for excessive data

  - Notification mechanisms, including messages to the system console, IDS tracing, and statistics
  - An action to reset the TCP connection when the send, receive, or out-of-order queue for the connection becomes constrained
- IDS provides the following enhancements to monitor IPv6 traffic:
  - Scan detection and reporting
  - Attack detection, reporting, and prevention
  - TCP and UDP traffic regulation
- If you are using IDS on a stack that is being run as a dual-mode stack (IPv4 and IPv6), new IPv6 monitoring and regulation will take effect automatically without any changes to policy in many cases. See IP Services: Understand and prepare for expanded Intrusion Detection Services in z/OS Migration for a detailed list of those cases.

The reports produced by the z/OS UNIX **trmdstat** command are updated to include new IDS information, such as new attack types.

Restriction: The new IDS policy configuration is provided only in a Policy Agent configuration file; the new configuration is not provided in Lightweight Directory Access Protocol (LDAP).

See "Intrusion detection services support for Enterprise Extender" on page 87 for information about the IDS support for Enterprise Extender (EE).

Using the expanded intrusion detection services

To use the expanded IDS, perform the appropriate tasks in Table 50.

Table 50. Expanded intrusion detection services

Task	Reference
Enable new IDS policies using IBM Configuration Assistant for z/OS Communications Server or manual configuration. • If you are using the Configuration Assistant, migrate your current backing store to V1R13. • Enable new attack types, as needed. • Enable an ICMPv6 scan rule, as needed. • Configure IPv6 addresses, as needed, in the scan exclusion list. • Configure IPv6 addresses, as needed, for traffic regulation.	• Intrusion detection services in z/OS Communications Server: IP Configuration Guide • IBM Configuration Assistant for z/OS Communications Server online help; see the "What's New in V1R13" help information for IDS configuration • IDS policies defined in IDS configuration files in z/OS Communications Server: IP Configuration Reference
Optionally, display policy-based networking information. Use the z/OS UNIX **pasearch** command to display IDS policies.	The z/OS UNIX pasearch command—Display policies in z/OS Communications Server: IP System Administrator's Commands
Generate reports that summarize or that provide detail about IDS events that have been detected on a stack. Use the z/OS UNIX **trmdstat** command to generate reports from a syslogd file with IDS messages.	The z/OS UNIX trmdstat command in z/OS Communications Server: IP System Administrator's Commands

Network address translation traversal support for IKE version 2

z/OS V1R13 Communications Server enhances the Internet Key Exchange daemon (IKED) to support Internet Key Exchange version 2 (IKEv2) network address

translation traversal (NATT) for IPv4 traffic. NATT occurs when IPSec protects traffic that traverses a NAT device. The IKEv2 protocol defined in RFC 5996 allows IPSec in specific cases to traverse one or more NAT devices. For information about how to access RFCs, see Appendix A, "Related protocol specifications," on page 91.

z/OS IKEv2 NATT and z/OS IKEv1 NATT have the same set of supported configurations. See the configuration scenarios supported for NAT traversal in z/OS Communications Server: IP Configuration Guide for information about the defined group of configurations that is supported.

Restrictions: The same restrictions that exist for z/OS IKEv1 NATT exist for z/OS IKEv2 NATT; see Configuration scenarios supported for NAT traversal in z/OS Communications Server: IP Configuration Guide for details.

Using network address translation traversal support for IKE version 2

To use the NATT support for IKE version 2, perform the appropriate tasks in Table 51.

Table 51. Network address translation traversal support for IKE version 2

Task	Reference
Modify IP security policy to allow NATT for IKEv2. To enable the IKE daemon to perform NATT using IKEv2, specify the value YES on the AllowNat parameter on the KeyExchangePolicy statement, the KeyExchangeAction statement, or on both statements, in the IPsec policy.	See the following topics in z/OS Communications Server: IP Configuration Reference: • KeyExchangePolicy statement • KeyExchangeAction statement
When you are using IBM Configuration Assistant for z/OS Communications Server, set the NATT default setting in the IPSec perspective stack settings. You can modify the NATT setting for each connectivity rule in the advanced settings for the rule.	IBM Configuration Assistant for z/OS Communications Server online help for the IPSec perspective stack settings

Sysplex-Wide Security Associations for IKE version 2

z/OS V1R13 Communications Server introduces support for IKEv2 in a Sysplex-Wide Security Association (SWSA) environment. SWSA provides better workload balancing for IPSec-protected workloads because it performs the following actions:

- Optimally routes new work to the target system and the server application, based on WLM advice
- Increases the availability of workloads by routing traffic around failed components
- Increases flexibility by adding additional workload in a nondisruptive manner

SWSA distributes the IPSec processing, including cryptography, for a single IPSec Security Association (SA) among systems in a sysplex environment. SWSA also allows workloads with IPSec-protected traffic to use the dynamic virtual IP address (DVIPA) takeover function. You can associate IPSec-protected workloads with DVIPAs that can be recovered by other systems in the case of a failure or planned takeover. IPSec SAs are automatically restarted on another system in the sysplex when a DVIPA takeover occurs.

Support for the Internet Key Exchange version 2 (IKEv2) protocol was provided in z/OS V1R12 Communications Server. The function provided in V1R12 did not include support for SWSA. SAs that were negotiated using the IKEv2 protocol

could not be distributed or taken over in a sysplex environment. Starting in z/OS V1R13, SAs protecting IPv4 traffic that is negotiated using the IKEv2 protocol can be distributed and taken over in a sysplex environment.

Restrictions:

- All target systems must be at V1R12 or later to participate in workload distribution for traffic over an IKEv2 tunnel.
- If the backup stack is on a system that is V1R12 or earlier, the IKE daemon attempts to negotiate a new SA using the IKEv1 protocol. Any SA that has been converted from IKEv2 to IKEv1 will continue to be renegotiated using the IKEv1 protocol for the life of the SA.

Using Sysplex-Wide Security Associations for IKE version 2

To use SWSA for IKEv2, perform the appropriate tasks in Table 52.

Table 52. Sysplex-Wide Security Associations for IKE version 2

Task	Reference
Learn about SWSA.	Sysplex-wide Security Associations and IP security in z/OS Communications Server: IP Configuration Guide
Enable SWSA by coding IPSEC DVIPSEC in the TCP/IP profiles of the distributor and backup stacks.	IPSEC statement in z/OS Communications Server: IP Configuration Reference
Display whether SWSA is enabled by using the **ipsec** command.	The ipsec command general report concepts in z/OS Communications Server: IP System Administrator's Commands

Improved security granularity for VIPARANGE DVIPAs

z/OS V1R13 Communications Server enhances application-specific dynamic virtual IP address (DVIPA) processing to provide more granular control over which users are allowed to create a specific IP address within a VIPARANGE statement. You can restrict which users can create or have access to a specific DVIPA or to a specific range of DVIPAs by using the existing System Authorization Facility resources. You can ensure that a particular DVIPA or DVIPA range is used only by a particular application.

Using the improved security granularity for VIPARANGE DVIPAs

To use the improved security granularity for VIPARANGE DVIPAs, perform the appropriate tasks in Table 53.

Table 53. Improved security granularity for VIPARANGE DVIPAs

Task	Reference
Define the following SAF resource profiles in the SERVAUTH class: • EZB.BINDDVIPARANGE.*sysname.tcpname.resname* • EZB.MODDVIPA.*sysname.tcpname.resname*	• TCP/IP resource protection in z/OS Communications Server: IP Configuration Guide • Defining a security profile for binding to DVIPAs in the VIPARANGE statement in z/OS Communications Server: IP Configuration Guide • Defining a security profile for SIOCSVIPA, SIOCSVIPA6, and MODDVIPA in z/OS Communications Server: IP Configuration Guide • EZARACF sample in SEZAINST
Specify the SAF keyword on the VIPARANGE statement.	VIPARANGE statement in z/OS Communications Server: IP Configuration Reference

Table 53. Improved security granularity for VIPARANGE DVIPAs (continued)

Task	Reference
Display the resource name (*resname*) and other configured DVIPA range information.	Netstat VIPADCFG/-F report in z/OS Communications Server: IP System Administrator's Commands

FTP support for password phrases

In z/OS V1R13 Communications Server, you can use password phrases when you log in to the z/OS FTP server. The password phrase is passed to the FTPCHKPWD exit routine if that user exit is installed.

You can also specify a password phrase instead of a password when you use the z/OS FTP client subcommands User and PAss.

Restrictions:

- RACF enforces a basic set of syntax rules to establish strength in password phrases. These syntax rules apply to all password phrases; you cannot alter or avoid them. However, you can add password phrase syntax rules to impose additional restrictions when your installation tailors the new password phrase exit (ICHPWX11).
- The password phrase that you use to log in to the z/OS FTP server has additional restrictions. The password phrase must not contain the following characters that have special meaning to the z/OS FTP server:
  - NULL (X'00')
  - slash (/)
  - colon (:)
  - carriage return (<cr>)
  - line feed (<lf>)
  - interpret as command (<IAC>) or X'FF')
  - Telnet command characters (X'FB' - X'FE')
- The password phrase must not contain leading blanks or trailing blanks.
- The maximum length of a password phrase is 100 characters.
- When you configure the z/OS FTP server for anonymous FTP, the following rules apply:
  - Do not specify a password phrase instead of a password as an FTP daemon start option.
  - Do not code a password phrase instead of a password on the ANONYMOUS statement in the FTP.DATA data set.

Dependency: To use this support, your security product must be SAF-compliant and it must support the use of password phrases as an alternative to passwords.

Coexistence requirement: The minimum length of a password phrase depends on whether you have installed the RACF exit ICHPWX11, or the equivalent exit for your SAF-compliant security product, and whether you have modified the exit to permit shorter password phrases.

- If you have not installed exit ICHPWX11, password phrases must be 14 -100 characters in length.
- When the new-password-phrase exit (ICHPWX11) is installed and is coded to allow shorter password phrases, the password phrase can be 9-100 characters in length.

Using FTP support for password phrases

To use the FTP support for password phrases, perform the appropriate tasks in Table 54.

Table 54. FTP support for password phrases

Task	Reference
Assign password phrases to user IDs that log in to the z/OS FTP server.	If the security product being used is RACF, see z/OS Security Server RACF Security Administrator's Guide
Learn about the ICHPWX11 exit routine.	z/OS Security Server RACF System Programmer's Guide
Configure the z/OS FTP server for anonymous FTP.	• Configuring the FTP server for anonymous FTP (optional) in z/OS Communications Server: IP Configuration Guide • FTP server cataloged procedure (FTPD) parameters in z/OS Communications Server: IP Configuration Reference
Inspect the password or password phrase that was used to log in to the z/OS FTP server before allowing the FTP server to use the information to authenticate the client.	• The FTCHKPWD user exit in z/OS Communications Server: IP Configuration Guide • The FTCHKPWD user exit in z/OS Communications Server: IP Configuration Reference
Code a password phrase in the NETRC data set or file of the z/OS FTP client.	NETRC data set in z/OS Communications Server: IP User's Guide and Commands
Specify a password phrase as an argument of the z/OS FTP client User or PAss subcommand.	See the following topics in z/OS Communications Server: IP User's Guide and Commands: • PAss subcommand • User subcommand
Specify a password phrase while you are logging in to any FTP server using the z/OS FTP client.	Logging in to FTP in z/OS Communications Server: IP User's Guide and Commands

Removed superuser requirement for Policy Agent and IKE daemon

Starting in z/OS V1R13 Communications Server, the Policy Agent and IKED servers can run without UID(0) or BPX.SUPERUSER authority. As in previous releases, the OMPROUTE and TN3270E servers can also run without UID(0) or BPX.SUPERUSER authority. z/OS Communications Server: IP Configuration Guide provides updated guidance about running servers without superuser authority.

Dependency: You must specify appropriate z/OS UNIX System Services file access authority for all files that are to be used by a server.

Removing the superuser requirement for Policy Agent and IKE daemon

If you consider the superuser authority [UID(0) or BPX.SUPERUSER] that is provided to your servers to be a security concern or if the number of UID(0) users as displayed by the z/OS UNIX System Services command **ps -U 0** is near the system limit, then perform the appropriate tasks in Table 55 to remove the superuser authority from the servers.

Table 55. Removed superuser requirement for Policy Agent and IKE daemon

Task	Reference
Remove the superuser authority [UID(0) or BPX.SUPERUSER] from the Policy Agent server.	Other considerations when starting the Policy Agent in z/OS Communications Server: IP Configuration Guide

Table 55. Removed superuser requirement for Policy Agent and IKE daemon (continued)

Task	Reference
Remove the superuser authority [UID(0) or BPX.SUPERUSER] from the TN3270E Telnet server.	Steps for defining security for a user ID and associating the user ID with the Telnet procedure name in z/OS Communications Server: IP Configuration Guide
Remove the superuser authority [UID(0) or BPX.SUPERUSER] from the OMPROUTE server.	Steps for configuring OMPROUTE in z/OS Communications Server: IP Configuration Guide
Remove the superuser authority [UID(0) or BPX.SUPERUSER] from the IKED server.	Steps for authorizing the IKE daemon to RACF in z/OS Communications Server: IP Configuration Guide

Enhanced IPsec support for FIPS 140 cryptographic mode

z/OS V1R13 Communications Server enhances Security Associations (SAs) distribution when the SAs are running in Federal Information Processing Standards (FIPS) 140 mode. When SAs running in FIPS mode are negotiated with the AES-GCM combined-mode encryption and authentication algorithm or with the AES-GMAC authentication algorithm, IPSec can distribute and take over the SAs in a Sysplex-Wide Security Association (SWSA) environment. IPSec-protected workloads that are using these algorithms can benefit from workload balancing with a sysplex.

The Internet Key Exchange (IKE) daemon can take advantage of new services that are provided by Integrated Cryptographic Service Facility (ICSF) when the IKE daemon is running in FIPS mode.

Restriction: All target systems must be at V1R12 or later to participate in workload distribution for traffic over a tunnel that is using AES-GCM or AES-GMAC in FIPS 140 mode.

Dependencies:

- If a V1R12 target system will be participating in the distributing workload of an UDP-encapsulated mode SA that was negotiated using the AES-GCM algorithm, then you must apply the V1R12 PTF for APAR PM29788. APAR PM29788 enables a target stack to handle decapsulated packets from the distributing stack when the packets were received over a UDP-encapsulated mode SA.
- If you run your IKE daemon in FIPS 140 mode, you must apply ICSF APAR OA34403.

Using the enhanced IPsec support for FIPS 140 cryptographic mode

The AES-GCM and AES-GMAC enhancements are automatically enabled; no tasks are necessary to use them. If your IKE daemon is running in FIPS mode, the IKE daemon enhancement requires you to perform the task in Table 56.

Table 56. Enhanced IPsec support for FIPS 140 cryptographic mode

Task	Reference
Permit the IKE daemon to the CSF1DVK and CSF1DMK resource profiles in the CSSERV class when IKE daemon is running in FIPS 140 mode.	Steps for setting up profiles in the CSFSERV resource class in z/OS Communications Server: IP Configuration Guide

Simplification

The following topics describe enhancements for simplification:

- "Configuration Assistant management of multiple z/OS Communications Server releases"
- "Configuration Assistant discovery of stack IP addresses"
- "Configuration Assistant common configuration of multiple stacks" on page 72
- "Configuration Assistant enhancements" on page 73
- "Wildcard support for the PORTRANGE statement" on page 74

Configuration Assistant management of multiple z/OS Communications Server releases

In z/OS V1R13 Communications Server, you can use IBM Configuration Assistant for z/OS Communications Server (Configuration Assistant) to configure multiple z/OS releases (V1R12 and V1R13). You can configure multiple LPARs that are running different releases by using a single instance of the Configuration Assistant.

Using Configuration Assistant to manage multiple releases

To use the Configuration Assistant to manage multiple z/OS Communications Server releases, perform the appropriate tasks in Table 57.

Table 57. Configuration Assistant management of multiple z/OS Communications Server releases

Task	Reference
Specify the z/OS release level for images (LPARs). When you create a new image by using the Configuration Assistant, specify the z/OS release level on the New z/OS Image panel. The default release level is the current release.	IBM Configuration Assistant online help
Change the z/OS release level for images (LPARs). To change the z/OS release level for an image by using the Configuration Assistant, click the image name in the navigation tree. Then select the z/OS release level from the drop-down list on the Image Information panel.	IBM Configuration Assistant online help

Configuration Assistant discovery of stack IP addresses

The IBM Configuration Assistant for z/OS (Configuration Assistant) makes it easier to create policy rules by discovering the local IP addresses for a TCP/IP stack and importing them into the Configuration Assistant. After you associate local addresses with the TCP/IP stack, you can use the addresses in IP address groups or in places that IP addresses are specified. By using the discovery function, you do not have to remember your IP addresses and manually enter them when you are creating rules or IP address groups.

Using Configuration Assistant discovery of stack IP addresses

To use the Configuration Assistant discovery of stack IP addresses, perform the appropriate tasks in Table 58.

Table 58. Configuration Assistant discovery of stack IP addresses

Task	Reference
Configure the Policy Agent to allow the discovery of TCP/IP profile information. Specify the ServicesConnection statement in the main Policy Agent configuration file.	• Policy-based networking in z/OS Communications Server: IP Configuration Guide • ServicesConnection in z/OS Communications Server: IP Configuration Reference

Table 58. Configuration Assistant discovery of stack IP addresses (continued)

Task	Reference
Enable AT-TLS for secure connections. Perform the following steps: 1. If you specify the Security Secure parameter on the ServicesConnection statement, enable AT-TLS processing for the TCP/IP stack by configuring the TTLS parameter on the TCPCONFIG statement in the TCP/IP profile. 2. Specify the affected TCP/IP stack by using the ImageName parameter on the ServicesConnection statement, or use the name specified (or specified by default) on the TCPIPUSERID statement or TCPIPJOBNAME statement in TCPIP.DATA. If the default TCP/IP image cannot be determined, the Policy Agent uses the image name INET.	• Application Transparent Transport Layer Security data protection in z/OS Communications Server: IP Configuration Guide • TCPCONFIG in z/OS Communications Server: IP Configuration Reference
Authorize the user IDs that the import requestors use to access the requested profile information. Issue security product commands to permit the import requestor user IDs to the following SERVAUTH profile: `EZB.PAGENT.`*`sysname.image.ptype`* The *image* value is the import request name used by the import requestor. For TCP/IP profile information, this name is the TCP/IP stack name specified on the TcpImage statement. Set the *ptype* value to CFGSERV or specify a wildcard value.	• Policy-based networking in z/OS Communications Server: IP Configuration Guide • Policy Agent general configuration file statements in z/OS Communications Server: IP Configuration Reference
Start Policy Agent from a started procedure or from the UNIX shell.	• Starting and stopping the Policy Agent in z/OS Communications Server: IP Configuration Guide • Policy Agent and policy applications in z/OS Communications Server: IP Configuration Reference
Import TCP/IP profile information into IBM Configuration Assistant for z/OS Communications Server. Perform the following steps: 1. Using the Configuration Assistant, create a new image and stack, or migrate the configuration backing store file from a previous release. 2. In the IPSec perspective, select a specific stack and click the **Local Addresses** tab. 3. On the **Local Addresses** tab, select **Discover...** from the **Select Action** menu. 4. Complete the information on the Discover Stack Local Addresses panel and click **Go**.	Select Help on the Discover Stack Local Addresses panel.

Table 58. Configuration Assistant discovery of stack IP addresses (continued)

Task	Reference
Force Policy Agent to listen for services requestor connections. Issue the MODIFY *procname*,SRVLSTN command in the following situations: • If you specified a TCP/IP stack using the ImageName parameter on the ServicesConnection statement (but you did not specify a TcpImage statement for the same TCP/IP stack), and the TCP/IP stack was not active when Policy Agent was started, issue the MODIFY command when the stack becomes active to restart the listen for services requestor connections. • If you retrieve AT-TLS policies from a policy server, but the policies cannot be retrieved immediately as a result of a network or policy server problem, issue the MODIFY command to reinstall the AT-TLS policy that was generated. Reinstalling the AT-TLS policy forces Policy Agent to listen for services requestor connections. • If you specified Security Secure on the ServicesConnection statement, the AT-TLS policy that was generated is installed successfully, and the key ring contents are changed but the key ring name is unchanged, issue the MODIFY command. Policy Agent reinstalls the AT-TLS policy that was generated so that the updated key ring changes are used.	ServicesConnection in z/OS Communications Server: IP Configuration Reference

Configuration Assistant common configuration of multiple stacks

Before z/OS V1R13 Communications Server, IP security administrators had to create a set of rules for each TCP/IP stack. Many of these rules were identical across stacks, and some settings were specific to the stack. An example of stack-specific settings is the settings for the stack's local addresses.

In z/OS V1R13 Communications Server, you can use the IBM Configuration Assistant for z/OS (Configuration Assistant) to create common configuration objects by using existing reusable configuration objects: address groups, traffic descriptors, security levels, and requirement maps, and new reusable rule configuration objects. By using reusable rules, you can reduce the number of configuration tasks that apply to multiple TCP/IP stacks. You can create a single rule and assign it to multiple stacks. You define the rule only once and you modify it in a single location. To make the rule reusable across TCP/IP stacks, you can use symbols or names. IP security rules are now reusable because you can configure the local addresses as a name, rather than as a specific IP address. These names resolve to the correct IP address on each stack to which you assign the rule.

Using the Configuration Assistant to configure multiple stacks

To use the Configuration Assistant to configure multiple stacks, perform the appropriate tasks in Table 59 on page 73.

Table 59. Configuration Assistant common configuration of multiple stacks

Task	Reference
For each TCP/IP stack, configure the set of local IP addresses and assign names to each address by doing one of the following tasks: • In the IPSec perspective, select a stack from the navigation tree. Click the **Local Addresses** tab. Click **Add** to add an IP address and assign a name to it. • If you are running z/OSMF, in the IPSec perspective, select a stack from the navigation tree. Click the **Local Addresses** tab. Select **Discover** from the **Select Action** table menu to query the TCP/IP stack and automatically populate the panel with the stack's local addresses.	IBM Configuration Assistant online help
Create reusable rules using IP address names by performing the following steps: 1. Select the Rules node in the navigation tree under the Reusable Objects tree node. 2. Click **Add** to create a new rule. For the local data endpoint, use the IP address name to represent the actual IP address.	IBM Configuration Assistant online help
Assign the new reusable rule to the stack by clicking on the stack in the navigation tree. Click **Add** to add the reusable rule to the stack. On the first panel in the rule wizard, add a reusable rule, and select the reusable rule you created. Complete the wizard.	IBM Configuration Assistant online help
Propagate to additional TCP/IP stacks by repeating these tasks for as many TCP/IP stack and reusable rules as necessary.	IBM Configuration Assistant online help

Configuration Assistant enhancements

In z/OS V1R13 Communications Server, the IBM Configuration Assistant for z/OS (Configuration Assistant) supports z/OSMF System Authorization Facility (SAF) mode authorization and registers the Configuration Assistant home page with the z/OSMF application linking function. You can use your security product instead of z/OSMF to authorize users. Other applications can link to z/OSMF applications.

In addition, you can do the following tasks:

- Use password phrases when you are using FTP from the Configuration Assistant
- Delete backing-store files when you are running in z/OSMF mode
- Enable a default AT-TLS rule to support the RACF Remote Sharing Facility (RRSF)

Restriction: You can delete backing-store files from z/OSMF only; you cannot delete backing-store files from the Windows client.

Using the Configuration Assistant enhancements

To use the Configuration Assistant enhancements, perform the appropriate tasks in Table 60 on page 74.

Table 60. Configuration Assistant enhancements

Task	Reference
Use SAF mode authorization for z/OSMF.	Setting up security for z/OSMF in IBM z/OS Management Facility Configuration Guide
Use password phrases when you are using FTP. Type the password phrase instead of a simple password on the FTP panel.	IBM Configuration Assistant online help for the FTP panel
Delete a backing-store file while you are using z/OSMF. From the Action menu, select **Open**, and then select **Open Existing Backing Store**. Highlight the backing-store file you want to delete and click the **Delete** tab.	IBM Configuration Assistant online help for the Select a Backing Store File panel
Enable AT-TLS for RRSF. From the AT-TLS perspective, select a stack, and then select the default RRSF rule and enable it.	IBM Configuration Assistant online help for the AT-TLS perspective connectivity rules panel

Wildcard support for the PORTRANGE statement

In z/OS V1R13 Communications Server, you can specify the job name on the PORTRANGE statement as a 1 - 7 character prefix followed by an asterisk (*). The wildcard setting allows several jobs with the same prefix to have access to the ports in the specified port range. You can use the wildcard setting on both TCP and UDP job names.

Using the wildcard support for the PORTRANGE statement

To use the wildcard support for the PORTRANGE statement, perform the task in Table 61.

Table 61. Wildcard support for the PORTRANGE statement

Task	Reference
Give jobs that have the same prefix access to a specified port range.	PORTRANGE statement in z/OS Communications Server: IP Configuration Reference

Dynamic infrastructure

The following topics describe enhancements for dynamic infrastructure:

- "HiperSockets optimization for intraensemble data networks"
- "Support for additional VLANs for an OSA-Express QDIO port" on page 75

HiperSockets optimization for intraensemble data networks

In z/OS V1R12 Communications Server, the IBM zEnterprise 196 (z196) offered communications access to two internal networks through OSA-Express3 adapters that were configured with an appropriate channel path ID (CHPID) type. One of the internal networks introduced in V1R12 was the intraensemble data network (IEDN). z/OS V1R13 Communications Server provides IEDN connectivity over HiperSockets; the IEDN traffic that is flowing to other LPARs that are in the same central processor complex (CPC) can use the HiperSockets connectivity instead of requiring the traffic to use the Ethernet LAN connectivity.

Restriction: Connectivity to the intraensemble data network is allowed only when the CPC is a member of an ensemble.

Dependencies:

- The V1R13 function requires an IBM zEnterprise 196 (z196) or IBM zEnterprise 114 (z114). See the 2817DEVICE and 2818DEVICE Preventive Service Planning (PSP) buckets for service information.
- This function requires an IQD CHPID that is configured with the Internal Queued Direct I/O extensions function (IQDX).
- This function is dependent on the z/OS LPAR participating in an ensemble. See *zEnterprise System Ensemble Planning and Configuring Guide* for more information.

Using the HiperSockets optimization for intraensemble data networks

To use the HiperSockets optimization for intraensemble data networks, perform the appropriate tasks in Table 62.

Table 62. HiperSockets optimization for intraensemble data networks

Task	Reference
Enable connectivity to the intraensemble data network.	TCP/IP in an ensemble in z/OS Communications Server: IP Configuration Guide
Configure an IQD CHPID with the Internal Queued Direct I/O extensions (IQDX) function in Hardware Configuration Definition (HCD).	
Display whether the stack is enabled for dynamic IQDX interfaces and whether the stack should use these interfaces for large outbound TCP socket data transmissions.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display information about the dynamic IQDX TRLEs and datapath devices by issuing the DISPLAY NET,ID=trle or DISPLAY NET,TRL,TRLE= command.	See the following topics in z/OS Communications Server: SNA Operation: • DISPLAY ID command • DISPLAY TRL command
Display information about an IQDX interface by issuing the Netstat DEvlinks/-d command against the IQDX interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display information about the number of packets and bytes for an OSX interface that went over the dynamic IQDX interface by issuing the Netstat DEvlinks/-d command against the OSX interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display the Address Resolution Protocol (ARP) cache entries associated with an IPv4 IQDX interface by issuing the Netstat ARp/-R command.	Netstat ARp/-R report in z/OS Communications Server: IP System Administrator's Commands
Display the neighbor cache entries associated with an IPv6 IQDX interface by issuing the Netstat ND/-n command.	Netstat ND/-n report in z/OS Communications Server: IP System Administrator's Commands

Support for additional VLANs for an OSA-Express QDIO port

z/OS V1R13 Communications Server increases the number of virtual local area networks (VLANs) that you can configure from the same TCP/IP stack for a single OSA-Express port.

The limit of supported IPv4 VLANs and IPv6 VLANs is increased from 8 to 32 VLANs per OSA-Express port.

Using the support for additional VLANs for an OSA-Express QDIO port

To use the support for additional VLANs for an OSA-Express QDIO port, perform the appropriate tasks in Table 63.

Table 63. Support for additional VLANs for an OSA-Express QDIO port

Task	Reference
Define additional VLANs for an OSA-Express port by configuring additional INTERFACE statements.	See the following statements in z/OS Communications Server: IP Configuration Reference: • INTERFACE — IPAQENET OSA-Express QDIO interfaces • INTERFACE — IPAQENET6 OSA-Express QDIO interfaces
Verify that the TRLE definition for the OSA-Express feature has sufficient DATAPATH devices for the number of VLANs that you have configured.	DATAPATH parameter of the TRLE definition statement in z/OS Communications Server: SNA Resource Definition Reference

Economics and platform efficiency

The following topics describe enhancements for economics and platform efficiency:

- "Increased CTRACE and VIT capacity"
- "OSA-Express4S QDIO IPv6 checksum and segmentation offload" on page 78

Increased CTRACE and VIT capacity

z/OS V1R13 Communications Server reduces ECSA storage by relocating the VTAM internal trace (VIT) table to 64-bit common (HVCOMMON) storage. You now specify the VIT table size in megabytes instead of in pages. The valid range for the table size is 4 - 2048 megabytes instead of 100 - 999 pages. The default size of the VIT table is 4 megabytes. The data space VIT function, including the VIT data space ISTITDS1, has been removed.

In z/OS V1R13 Communications Server, the component trace records in the TCP/IP data space TCPIPDS1 have been relocated to 64-bit common (HVCOMMON) storage. The maximum size that you can specify as the value of the BUFSIZE() parameter has been increased from 256 megabytes (256M) to 1024 megabytes (1024M) for the CTRACE component SYSTCPIP. The DISPLAY TCPIP,*procname*,STOR and the DISPLAY TCPIP,*tnproc*,STOR commands can display 31-bit and 64-bit storage allocation.

Incompatibilities:

- You cannot use VTAM dump analysis tools from previous releases on dumps that you create in z/OS V1R13 or later releases.
- You cannot use V1R13 TCP dump analysis tools on dumps that you created in previous releases.
- You cannot use TCP dump analysis tools from previous releases on dumps that you create in z/OS V1R13 or later releases.

Tip: You no longer need to specify DSPNAME='*tcpname*'.TCPIPDS1 on the DUMP command.

Dependency: Storage for the component trace and the VIT table will not be allocated unless you have configured sufficient 64-bit common (HVCOMMON) storage. Configure the appropriate amount of 64-bit common (HVCOMMON)

storage by using the HVCOMMON parameter on the IEASYSxx parmlib member of SYS1.PARMLIB. See z/OS MVS Initialization and Tuning Reference for more information.

Using the increased CTRACE and VIT capacity

This function is automatically enabled; you are not required to perform configuration tasks to enable the new function. Your system will behave differently than it did previously; for example, you will receive informational messages and automation might yield unexpected results. You can perform the tasks in Table 64 to reduce or eliminate any unwanted changes in system behavior, to increase the size of your VIT table, or to specify a larger buffer size for the CTRACE component SYSTCPIP.

See z/OS Migration for complete migration details.

Table 64. Increased CTRACE and VIT capacity

Task	Reference
Prevent start option informational messages from being issued by updating your VTAM start option list (ATCSTRxx). Prevent the automated MODIFY TRACE command from failing by updating your automation. • If the SIZE parameter is specified, convert the value to megabytes. • If the DSPSIZE parameter is specified, delete the DSPSIZE specification.	Adjust to the relocation of the VTAM internal trace table in z/OS Migration
Prevent other automation failures by ensuring that the automation does not expect any of the newly retired messages.	Adjust to the relocation of the VTAM internal trace table in z/OS Migration
Increase the size of your VIT table by performing the following steps: 1. Determine the new size of your VIT in megabytes. **Restriction:** If you specify a SIZE value that is larger than the default value, z/OS will perform paging on portions of the VIT table. Before you specify a large SIZE value, ensure that you have sufficient real or auxiliary storage to contain the entire VIT. Failure to ensure sufficient storage might result in an auxiliary storage shortage. If an SVC dump is taken that includes common storage, the size of the dump data set also increases. You must also take the increase in the size of the dump data set into consideration. 2. In order for the new size value to be applied every time VTAM is started, you must specify the new value on the SIZE operand of the TRACE start option in your VTAM start option list (ATCSTRxx). 3. You can temporarily apply the new size value to last as long as VTAM is active. To do this, specify the new value on the SIZE parameter of the MODIFY TRACE command. 4. Ensure the new size value is in effect by issuing the DISPLAY NET,TRACES command. Check the size as reported at the end of message IST315I.	• 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

Table 64. Increased CTRACE and VIT capacity (continued)

Task	Reference
Specify a larger buffer size for the CTRACE component SYSTCPIP. Code the TRACE CT command and specify a value up to 1024 megabytes (1024M) for the SYS1.PARMLIB member CTIEZBxx or use the command TRACE CT,nnnM,COMP=SYSTCPIP,SUB=(*procedure_jobname*).	Modifying options with the TRACE CT command in z/OS Communications Server: IP Diagnosis Guide

OSA-Express4S QDIO IPv6 checksum and segmentation offload

z/OS V1R13 Communications Server improves IPv6 performance and reduces processor usage by extending the checksum offload and segmentation offload functions to IPv6 OSA-Express4S interfaces that are running in QDIO mode. The z/OS stack also offloads IPv4 and IPv6 checksum processing for packets that flow between stacks that share the same OSA port. IPv6 checksum offload is enabled by default for OSA-Express4S features that support checksum offloading. IPv6 segmentation offload is disabled by default; you can enable it by specifying the IPCONFIG6 profile statement.

Restrictions:

- Checksum offload is limited to TCP and UDP packets.
- Checksum offload does not apply to outbound multicast packets.
- Segmentation offload is limited to TCP packets.
- Segmentation offload does not apply to packets that go to another stack that shares the OSA port.
- Checksum offload and segmentation offload do not apply to IPSec-encapsulated packets.
- Checksum offload and segmentation offload do not apply to IPv6 packets that contain extension headers.
- Checksum offload and segmentation offload do not apply when multipath is in effect unless all interfaces in the multipath group provide the same offload capabilities.

Dependencies:

- The checksum offload and segmentation offload enhancements are limited to OSA-Express4S or later Ethernet features that are configured with a CHPID type of OSD or OSX. See the 2817DEVICE and 2818DEVICE Preventive Service Planning (PSP) buckets for more information.
- Segmentation offload requires that you enable checksum offload.

Using OSA-Express4S QDIO IPv6 checksum and segmentation offload

To use the OSA-Express4S QDIO IPv6 checksum and segmentation offload, perform the appropriate tasks in Table 65.

Table 65. OSA-Express4S QDIO IPv6 checksum and segmentation offload

Task	Reference
Display whether checksum offload is enabled for an OSA-Express QDIO interface by issuing the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

Table 65. OSA-Express4S QDIO IPv6 checksum and segmentation offload (continued)

Task	Reference
Display whether checksum offload is globally enabled for OSA-Express QDIO IPv4 or IPv6 interfaces by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display whether segmentation offload is enabled for an OSA-Express QDIO interface by issuing the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Enable IPv6 segmentation offload by specifying the SEGMENTATIONOFFLOAD parameter on the IPCONFIG6 statement.	IPCONFIG6 statement in z/OS Communications Server: IP Configuration Reference
Enable IPv4 segmentation offload by specifying the SEGMENTATIONOFFLOAD parameter on the IPCONFIG statement. If the SEGMENTATIONOFFLOAD parameter is specified on the GLOBALCONFIG statement, move this setting to the IPCONFIG statement; this parameter on GLOBALCONFIG is deprecated.	See the following statements in z/OS Communications Server: IP Configuration Reference: • IPCONFIG • GLOBALCONFIG
Display whether segmentation offload is globally enabled for OSA-Express QDIO IPv4 or IPv6 interfaces by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands

Availability

The following topics describe enhancements for availability:

- "System resolver autonomic quiescing of unresponsive name servers"
- "Improved convergence for sysplex distribution routing when joining a sysplex" on page 80
- "CSSMTP extended retry" on page 80
- "Monitor CSM constrained conditions for sysplex autonomics" on page 81

System resolver autonomic quiescing of unresponsive name servers

In z/OS V1R13 Communications Server, the system resolver can dynamically stop using unresponsive Domain Name System (DNS) name servers and can resume using those name servers when they become responsive to resolver DNS polling queries. Name server responsiveness is determined by comparing the percentage of queries that are not responded to by the name server during regular intervals against a user specifiable threshold value.

Restriction: You must use a global TCPIP.DATA file if you want the resolver to dynamically stop using unresponsive name servers.

Using the system resolver autonomic quiescing of unresponsive name servers

To use the system resolver autonomic quiescing of unresponsive name servers, perform the appropriate tasks in Table 66 on page 80.

Table 66. System resolver autonomic quiescing of unresponsive name servers

Task	Reference
If you have not customized the resolver, create a resolver setup file and the resolver address space.	See the following topics in z/OS Communications Server: IP Configuration Guide: • Steps for creating a resolver setup file • Steps for defining the resolver address space
If you have not used a global TCPIP.DATA file, perform the following steps: 1. Create a global TCPIP.DATA file. 2. At a minimum, code the IP addresses of the name servers to be used for resolver queries in the global TCPIP.DATA file. 3. Code the GLOBALTCPIPDATA setup statement in the resolver setup file and specify the name of the global TCPIP.DATA file as the statement value.	• The resolver and the global TCPIP.DATA file in z/OS Communications Server: IP Configuration Guide • See the following topics in z/OS Communications Server: IP Configuration Reference: – NSINTERADDR statement – GLOBALTCPIPDATA statement
Determine the appropriate name server responsiveness threshold percentage to use initially for your environment. If you use the autonomic quiescing of the unresponsive name server function, you must code a value for the percentage parameter on the UNRESPONSIVETHRESHOLD setup statement because this has no default value.	Optimizing the UNRESPONSIVETHRESHOLD value for your network in z/OS Communications Server: IP Configuration Guide
Code the UNRESPONSIVETHRESHOLD (*percentage*,AUTOQUIESCE) setup statement in the resolver setup file.	UNRESPONSIVETHRESHOLD statement in z/OS Communications Server: IP Configuration Reference
If the resolver is not already started, start the resolver address space. If the resolver is already started, issue the MODIFY *resolver*,REFRESH,SETUP=*setup_file_name* command to enable the autonomic quiescing function: • Verify that message EZZ9304I AUTOQUIESCE is in the command output. • Verify that the list of name servers in the global TCPIP.DATA file is in message EZD2035I in the command output.	• See the following topics in z/OS Communications Server: IP Configuration Guide: – Starting the resolver – Managing the resolver address space • MODIFY command -- Resolver address space in z/OS Communications Server: IP System Administrator's Commands

Improved convergence for sysplex distribution routing when joining a sysplex

z/OS V1R13 Communications Server enhances the sysplex distributor VIPAROUTE function to make it more responsive to changes in the routing topology. This enhancement improves responsiveness of distributed dynamic virtual IP address (DVIPA) connections during TCP/IP initialization, when TCP/IP rejoins a sysplex group, or while OMPROUTE is being recycled.

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

CSSMTP extended retry

z/OS V1R13 Communications Server Simple Mail Transfer Protocol (CSSMTP) supports an extended retry function. If this function is enabled and CSSMTP exhausts the number of retries that is configured for a mail message, the message is written into a file on the z/OS UNIX file system and CSSMTP makes additional extended retries. The JES spool file that contains the message and the CSSMTP memory that holds the message are released during the extended retry time

period. You can configure the extended retry time period separately from long retry time period. The allowable time period is increased.

Using CSSMTP extended retry

To use the CSSMTP extended retry, perform the appropriate tasks in Table 67.

Table 67. CSSMTP extended retry

Task	Reference
Specify the ExtendedRetry statement to define the duration of the retry age, interval, and the name of the z/OS UNIX file system directory. CSSMTP extended retry is disabled by default.	ExtendedRetry statement in z/OS Communications Server: IP Configuration Reference
Flush messages from the extended retry directory, based on the age of the messages.	MODIFY FLUSHRetry,AGE in z/OS Communications Server: IP System Administrator's Commands

Monitor CSM constrained conditions for sysplex autonomics

z/OS V1R13 Communications Server includes enhanced sysplex monitoring that detects whether communications storage manager (CSM) is constrained for multiple monitoring intervals. If CSM is constrained, especially for long durations, packets might be dropped, which can have an adverse effect on transactions that reach the system image. When sysplex monitoring detects that CSM is constrained for multiple monitoring intervals, you can configure the stack to perform recovery actions similar to those taken when CSM is in a critical state.

Monitoring CSM constrained conditions for sysplex autonomics

To use the enhanced monitoring of CSM usage for sysplex autonomics, perform the task in Table 68.

Table 68. Monitor CSM constrained conditions for sysplex autonomics

Task	Reference
Specify the RECOVERY option on the SYSPLEXMONITOR parameter of the GLOBALCONFIG statement.	Sysplex problem detection and recovery in z/OS Communications Server: IP Configuration Guide

Application, middleware, and workload enablement

The following topics describe enhancements to application, middleware, and workload enablement:

- "Enhanced FTP support for extended address volumes" on page 82
- "FTP support for large-format data sets" on page 82
- "NMI for retrieving system resolver configuration information" on page 83
- "Simplified authorization requirements for real-time TCP/IP network monitoring NMI" on page 83
- "Enhancements to the TN3270E server" on page 84
- "CSSMTP enhancements" on page 85
- "Support for bypassing host name lookup in otelnetd" on page 85
- "TCP/IP serviceability enhancements" on page 86

Enhanced FTP support for extended address volumes

The z/OS FTP client and server support allocating data sets that are eligible for extended addressing space (EAS). You can transfer data to and from the following types of EAS-eligible data sets:

- Sequential data sets (basic, extended, and large formats)
- Partitioned data sets and extended partitioned data sets

You can configure FTP to allocate new MVS data sets as eligible for EAS.

Restrictions:

- You cannot allocate z/OS UNIX files as EAS-eligible files.

Dependency: DS8000® Licensed Internal Code 4.0 or higher is required to support extended address volumes (EAVs).

Using the enhanced FTP support for extended address volumes

To use the enhanced FTP support for extended address volumes, perform the appropriate tasks in Table 69.

Table 69. Enhanced FTP support for extended address volumes

Task	Reference
Learn about extended address volumes and EAS-eligible data sets.	z/OS DFSMS Using the New Functions
Configure FTP to allocate new MVS data sets with extended attributes.	• See the following topics in z/OS Communications Server: IP User's Guide and Commands: – LOCSIte subcommand – SIte subcommand – Dynamic allocation of new data sets • EATTR statement (FTP client and server) in z/OS Communications Server: IP Configuration Reference
Learn whether new data sets will be allocated with extended attributes.	See the following topics in z/OS Communications Server: IP User's Guide and Commands: • LOCSTat subcommand • STAtus subcommand

FTP support for large-format data sets

z/OS V1R13 Communications Server for z/OS FTP supports transfer to and from physical sequential large format data sets. You can configure FTP to allocate new physical sequential data sets as physical sequential basic format data sets or as physical sequential large-format data sets.

Restriction: The LIST command reply cannot always display accurate size information when it reports information about large data sets. When FTP cannot provide accurate size information, affected fields display a plus sign (+) to indicate that the actual size is larger than the LIST command reply can represent.

z/OS V1R13 Communications Server for z/OS FTP also supports transfer to and from z/OS UNIX files that are as large as or larger than two gigabytes.

Using the FTP support for large-format data sets

To use FTP transfer to and from physical sequential large format data sets, perform the appropriate tasks in Table 70 on page 83. No tasks are necessary to enable the

support for the transfer of z/OS UNIX files that are as large as or larger than two gigabytes; that support is automatically enabled.

Table 70. FTP support for large-format data sets

Task	Reference
Configure the FTP client or server to allocate new physical sequential data sets as physical sequential large-format data sets.	• DSNTYPE (FTP client and server) statement in z/OS Communications Server: IP Configuration Reference • See the DSNTYPE parameter description in the following topics in z/OS Communications Server: IP User's Guide and Commands: – LOCSIte subcommand – SIte subcommand
Determine whether the FTP client allocates new physical sequential data sets as physical sequential large-format data sets or as physical sequential basic format data sets.	LOCSTat subcommand in z/OS Communications Server: IP User's Guide and Commands
Determine whether the FTP server allocates new physical sequential data sets as physical sequential large-format data sets or as physical sequential basic format data sets.	STAtus subcommand in z/OS Communications Server: IP User's Guide and Commands

NMI for retrieving system resolver configuration information

z/OS V1R13 Communications Server provides resolver configuration information in response to a GetResolverConfig request that is sent on the new resolver callable NMI request (EZBREIFR). The resolver returns the resolver setup definitions and the resolver-related contents of the TCPIP.DATA file that were specified on the GLOBALTCPIPDATA resolver setup statement, if this information is specified.

Using the NMI for retrieving system resolver configuration information

The network management interface (NMI) for retrieving system resolver configuration information is automatically enabled. To use this NMI, perform the task in Table 71.

Table 71. NMI for retrieving system resolver configuration information

Task	Reference
Develop or enhance an application to obtain resolver configuration information using the resolver callable NMI.	Resolver NMI (EZBREIFR) in z/OS Communications Server: IP Programmer's Guide and Reference

Simplified authorization requirements for real-time TCP/IP network monitoring NMI

The real-time TCP/IP network monitoring network management interface (NMI) provides real-time data that network management applications can obtain. This NMI comprises the following service interfaces:

SYSTCPDA
TCP/IP packet and data trace data

SYSTCPCN
TCP connection SMF data

SYSTCPOT
OSAENTA trace data

SYSTCPSM
SMF data

Applications use the TMI copy buffer interface of the NMI to copy the real-time data to the application storage.

As of z/OS V1R13 Communications Server, network management applications that use this NMI are no longer required to be APF authorized to call the TMI copy buffer interface to copy the real-time data to the application storage. If an application is not APF authorized, the administrator must define the security product resource profiles of the real-time interface that the application is using and give the user ID of the application READ access to the resources.

Using the simplified authorization requirements for real-time TCP/IP network monitoring NMI

To use the simplified authorization requirements for real-time TCP/IP network monitoring NMI, perform the task in Table 72.

Table 72. Simplified authorization requirements for real-time TCP/IP network monitoring NMI

Task	Reference
Enable applications that are not APF authorized to use the TMI copy buffer interface for the real-time TCP/IP network monitoring NMI.	Real-time TCP/IP network monitoring NMI: Configuration and enablement in z/OS Communications Server: IP Programmer's Guide and Reference

Enhancements to the TN3270E server

z/OS V1R13 Communications Server provides a new operator command, DISPLAY TCPIP,TELNET. This command displays summary information such as the name, version, and state for all of the TN3270E Telnet servers that are or were active.

z/OS V1R13 Communications Server provides a new option, PASSWORDPHRASE, that allows the TN3270E Telnet server to accept either a password phrase or a password on the solicitor screen. When the new option is specified and you enter a new password or password phrase, you are asked to verify the new entry. Without the new option, new password verification is not requested.

The TN3270E server can dynamically adjust input buffer size based on the amount of data that is received. Dynamically adjusting the buffer size improves the performance of TN3270 connections that receive large messages.

Using the enhancements to the TN3270E server

To use the new DISPLAY TCPIP,TELNET command or the PASSWORDPHRASE option, perform the tasks in Table 73. There are no tasks to enable the support for the dynamically adjusted input buffer; it is automatically enabled.

Table 73. Enhancements to the TN3270E server

Task	Reference
Issue the DISPLAY TCPIP,TELNET command to show the status of all the TN3270E Telnet servers that are active or that were active.	• DISPLAY TCPIP,TELNET in z/OS Communications Server: IP System Administrator's Commands • EZAOP60I in z/OS Communications Server: IP Messages Volume 1 (EZA)
Enable users to enter a password phrase on the TN3270E Telnet server solicitor screen.	PASSWORDPHRASE statement in z/OS Communications Server: IP Configuration Reference

CSSMTP enhancements

In z/OS V1R13 Communications Server, you can customize the number of syntax errors that are allowed per spool file while Communications Server Simple Mail Transfer Protocol (CSSMTP) is parsing the spool file. If the allowed number of syntax errors is exceeded, then the spool file processing stops.

For the CSSMTP configuration file and spool files, you can use any EBCDIC single-byte code page that is supported by z/OS Unicode Services as long as the code page supports translations to and from IBM-1047 and ISO-8859-1. See z/OS Unicode Services User's Guide and Reference for more information about Unicode Services.

Dependency: z/OS Unicode Services must be active for the code pages used. The code pages must have translations for IBM-1047 (EBCDIC) and ISO8859-1 (ASCII).

Using the CSSMTP enhancements

To use the CSSMTP enhancements, perform the tasks in Table 74

Table 74. CSSMTP enhancements

Task	Reference
Change the number of syntax errors allowed by updating the CSSMTP configuration file and adding the JESSyntaxErrLimit statement.	JESSyntaxErrLimit statement in z/OS Communications Server: IP Configuration Reference
Update the environment variable CSSMTP_CODEPAGE_CONFIG to indicate the code page used for the configuration file.	See the following topics in z/OS Communications Server: IP Configuration Reference: • CSSMTP environment variables • CSSMTP sample started procedure
Update the TRANSLATE statement in the CSSMTP configuration statements to indicate the code page used for spool files.	CSSMTP configuration statements in z/OS Communications Server: IP Configuration Reference

Support for bypassing host name lookup in otelnetd

In z/OS V1R13 Communications Server, the z/OS UNIX Telnet server (otelnetd) has a new parameter that controls the lookups of the gethostbyaddr and getnameinfo routines. If you specify the new -g parameter, otelnetd will not issue the gethostbyaddr or getnameinfo routines to resolve the client IP address. If the domain name server (DNS) is not responding to the resolver in a timely manner, you can use the new otelnetd parameter to avoid delays in connecting to otelnetd caused by the hostname lookup.

Restriction: The -g parameter is ignored when the -U parameter is specified. The -U parameter causes otelnetd to drop connections from any IP address that cannot be mapped back into a symbolic name by the gethostbyaddr or getnameinfo routines.

Using the support for bypassing host name lookup in otelnetd

To use the support for bypassing host name lookup in otelnetd, perform the task in Table 75 on page 86

Table 75. Support for bypassing host name lookup in otelnetd

Task	Reference
Disable the z/OS UNIX Telnet server (otelnetd) from issuing the gethostbyaddr routine or the getnameinfo routine to resolve the client host name from the client IP address.	otelnetd in z/OS Communications Server: IP Configuration Guide

TCP/IP serviceability enhancements

z/OS V1R13 Communications Server provides the following TCP/IP serviceability enhancements:

- Support for logging traces of common formatting routines when the routines are called by the SNMP manager API
- Improved debugging for the z/OS UNIX System Services snmp command-line interface. Each level of debug output includes the output from lower levels of debugging.
- Enhanced reports from OMPROUTE console commands that include the source of the router ID definition that uniquely identifies a 32-bit router ID in an OSPF autonomous system

Using the TCP/IP serviceability enhancements

To use the TCP/IP serviceability enhancements, perform the appropriate tasks in Table 76.

Table 76. TCP/IP serviceability enhancements

Task	Reference
Enable logging of packet processing under the SNMP manager API by using the new SNMP logging level SNMP_LOG_INTERNAL.	See the following topics in z/OS Communications Server: IP Programmer's Guide and Reference: • snmpSetLogLevel • debugging the SNMP manager API
Activate any trace debug level, 1 through 4, using the -d parameter on the z/OS UNIX System Services **snmp** command.	z/OS UNIX snmp command in z/OS Communications Server: IP System Administrator's Commands
Use one or more of the following commands to display the IPv4 or IPv6 RouterID configuration source: • DISPLAY TCPIP,,OMPROUTE,OSPF,STATISTICS • DISPLAY TCPIP,,OMPROUTE,IPV6OSPF,ALL • MODIFY OMPROUTE,OSPF,STATISTICS • MODIFY OMPROUTE,IPV6OSPF,ALL	See the following topics in z/OS Communications Server: IP System Administrator's Commands: • DISPLAY TCPIP,,OMPROUTE • MODIFY OMPROUTE

SNA and Enterprise Extender

The following topics describe enhancements for SNA and Enterprise Extender (EE):

- "Intrusion detection services support for Enterprise Extender" on page 87
- "Enterprise Extender firewall-friendly connectivity test" on page 87
- "HPR packet trace analyzer for Enterprise Extender" on page 88
- "Improved APPN routing resilience" on page 88
- "Performance improvements for Enterprise Extender traffic" on page 88

Intrusion detection services support for Enterprise Extender

In z/OS V1R13 Communications Server, intrusion detection services (IDS) can monitor and protect Enterprise Extender (EE) traffic. Events are detected for IPv4 and IPv6 traffic.

Restriction: The new IDS policy configuration is provided only in a Policy Agent configuration file, not in Lightweight Directory Access Protocol (LDAP).

Using intrusion detection services support for Enterprise Extender

To use the IDS support for EE, perform the appropriate tasks in Table 77.

Table 77. Intrusion detection services support for Enterprise Extender

Task	Reference
Enable new IDS policies using the IBM Configuration Assistant for z/OS or manual configuration. 1. If you are using the Configuration Assistant, migrate your current backing store to V1R13. 2. Enable new attack types, as needed.	• IBM Configuration Assistant for z/OS Communications Server online help; see the "What's New in V1R13" help information for IDS configuration • IDS policies defined in IDS configuration files in z/OS Communications Server: IP Configuration Reference
Generate reports that summarize or provide detail about IDS events detected on a stack. Use the z/OS UNIX **trmdstat** command to generate reports from a syslogd file that contains IDS messages.	z/OS UNIX trmdstat command in z/OS Communications Server: IP System Administrator's Commands

Enterprise Extender firewall-friendly connectivity test

In z/OS V1R13 Communications Server, the DISPLAY NET,EEDIAG,TEST=YES,LIST=SUMMARY command output does not provide detailed routing information for Enterprise Extender (EE) connections. Instead, command processing expedites the EE connectivity test results. Quicker results might be beneficial to you if your IP configuration includes firewalls that block Internet Control Message Protocol (ICMP) messages, which results in delayed EE connectivity test results. The DISPLAY NET,EEDIAG,TEST=YES,LIST=SUMMARY command does not require ICMP messages to flow to verify basic EE connectivity. The DISPLAY NET, EEDIAG,TEST=YES,LIST=DETAIL has not changed; it still requires ICMP messages to flow in order to display the routing information for the EE connection.

Using the Enterprise Extender firewall-friendly connectivity test

To use the EE firewall-friendly connectivity test, perform the appropriate tasks in Table 78.

Table 78. Enterprise Extender firewall-friendly connectivity test

Task	Reference
To perform a quick EE connectivity test to verify basic connectivity between two EE endpoints, issue a DISPLAY NET,EEDIAG,TEST=YES,LIST=SUMMARY command.	DISPLAY EEDIAG command in z/OS Communications Server: SNA Operation
To perform an EE connectivity test to verify basic connectivity and provide detailed routing information between two EE endpoints, issue the DISPLAY NET,EEDIAG,TEST=YES,LIST=DETAIL command.	DISPLAY EEDIAG command in z/OS Communications Server: SNA Operation

HPR packet trace analyzer for Enterprise Extender

z/OS V1R13 Communications Server TCP/IP packet trace formatting provides new statistics for High-Performance Routing (HPR) traffic. The HPR packet trace analyzer for Enterprise Extender displays the following statistics for each transport connection identifier (TCID):

- Number of packets and bytes
- Out-of-order packets and bytes
- Number of packets and bytes retransmitted
- Number of ARB slowdowns
- Total elapsed time in ARB slowdown mode

You can access this report by selecting the HPRDIAG(SUMMARY) packet trace option of SYSTCPDA in Interactive Problem Control System (IPCS).

Using the HPR packet trace analyzer for Enterprise Extender

To use the HPR packet trace analyzer for EE, perform the task in Table 79.

Table 79. HPR packet trace analyzer for Enterprise Extender

Task	Reference
Format the new HPR report. Issue the new HPRDIAG option report on the packet trace data that was collected.	OPTIONS syntax in z/OS Communications Server: IP Diagnosis Guide
Obtain the new HPR report programmatically.	Passing options to the packet trace formatter in z/OS Communications Server: IP Programmer's Guide and Reference

Improved APPN routing resilience

z/OS V1R13 Communications Server processing provides autonomic recovery from Advanced Peer-to-Peer Networking (APPN) routing tree corruption. By issuing an operator command, you can also manually recover when routes are consistently selected incorrectly.

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

Performance improvements for Enterprise Extender traffic

In z/OS V1R13 Communications Server, processing for OSA-Express in QDIO mode supports inbound workload queueing for Enterprise Extender (EE) workloads. Inbound workload queueing uses multiple input queues for each QDIO data device (subchannel device) to improve TCP/IP stack scalability and general network optimization. To implement the performance improvements for EE workloads, enable inbound workload queueing to process EE, sysplex distributor, and streaming bulk data traffic all concurrently with other types of inbound QDIO traffic. When you enable these improvements for a QDIO interface, then inbound EE, sysplex distributor, and streaming bulk data traffic are each processed on their own ancillary input queue (AIQ). All other inbound traffic is processed on the primary input queue.

Restrictions:

- This function is not supported when z/OS V1R13 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.

- Additional CSM 4K DSPACE64 storage is used when the QDIO inbound workload queue is implemented. Display the VTAM TRLE name associated with the device to determine the amount of CSM storage that is used.

Incompatibility: 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 or later in QDIO mode running on the IBM zEnterprise 196 (z196) or IBM zEnterprise 114 (Z114).. For more information about the QDIO inbound workload queueing function and the OSA-Express features that support it, see QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide.
- See the 2817DEVICE and 2818DEVICE Preventive Service Planning (PSP) buckets for service information.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

Using the performance improvements for Enterprise Extender traffic

To use the performance improvements for EE traffic, perform the appropriate tasks in Table 80.

Table 80. Performance improvements for Enterprise Extender traffic

Task	Reference
Enable inbound workload queueing for a specific QDIO interface by specifying the WORKLOADQ parameter 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.	• See the following statements in z/OS Communications Server: IP Configuration Reference: – INTERFACE - IPAQENET OSA-Express QDIO interfaces – INTERFACE - IPAQENET6 OSA-Express QDIO interfaces • 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 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.	See the following topics in z/OS Communications Server: SNA Operation: • DISPLAY ID command • DISPLAY TRL command
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by initiating VTAM tuning statistics for the QDIO interface.	MODIFY TNSTAT command in z/OS Communications Server: SNA Operation
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by using the TCP/IP callable NMI GetIfStatsExtended request.	TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer's Guide and Reference

Table 80. Performance improvements for Enterprise Extender traffic (continued)

Task	Reference
Determine the QID on which a specific packet was received, and the associated workload queueing function, from a packet trace.	Formatting packet traces using IPCS in z/OS Communications Server: IP Diagnosis Guide
Determine the QID on which a specific packet was received from an OSAENTA trace.	Formatting OSA traces using IPCS in z/OS Communications Server: IP Diagnosis Guide

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.

Draft RFCs that have been implemented in this and previous Communications Server releases are listed at the end of this topic.

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

RFC Title and Author

RFC 652
Telnet output carriage-return disposition option D. Crocker

RFC 653
Telnet output horizontal tabstops option D. Crocker

RFC 654
Telnet output horizontal tab disposition option D. Crocker

RFC 655
Telnet output formfeed disposition option D. Crocker

RFC 657
Telnet output vertical tab disposition option D. Crocker

RFC 658
Telnet output linefeed disposition D. Crocker

RFC 698
Telnet extended ASCII option T. Mock

RFC 726
Remote Controlled Transmission and Echoing Telnet option J. Postel, D. Crocker

RFC 727
Telnet logout option M.R. Crispin

RFC 732
Telnet Data Entry Terminal option J.D. Day

RFC 733
Standard for the format of ARPA network text messages D. Crocker, J. Vittal, K.T. Pogran, D.A. Henderson

RFC 734
SUPDUP Protocol M.R. Crispin

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

RFC 736
Telnet SUPDUP option M.R. Crispin

RFC 749
Telnet SUPDUP—Output option B. Greenberg

RFC 765
File Transfer Protocol specification J. Postel

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 3826
The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model U. Blumenthal, F. Maino, K McCloghrie.

RFC 3947
Negotiation of NAT-Traversal in the IKE T. Kivinen, B. Swander, A. Huttunen, V. Volpe

RFC 3948
UDP Encapsulation of IPsec ESP Packets A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg

RFC 4001
Textual Conventions for Internet Network Addresses M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 4007
IPv6 Scoped Address Architecture S. Deering, B. Haberman, T. Jinmei, E. Nordmark, B. Zill

RFC 4022
Management Information Base for the Transmission Control Protocol (TCP) R. Raghunarayan

RFC 4106
The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) J. Viega, D. McGrew

RFC 4109
Algorithms for Internet Key Exchange version 1 (IKEv1) P. Hoffman

RFC 4113
Management Information Base for the User Datagram Protocol (UDP) B. Fenner, J. Flick

RFC 4191
Default Router Preferences and More-Specific Routes R. Draves, D. Thaler

RFC 4217
Securing FTP with TLS P. Ford-Hutchinson

RFC 4292
IP Forwarding Table MIB B. Haberman

RFC 4293
Management Information Base for the Internet Protocol (IP) S. Routhier

RFC 4301
Security Architecture for the Internet Protocol S. Kent, K. Seo

RFC 4302
IP Authentication Header S. Kent

RFC 4303
IP Encapsulating Security Payload (ESP) S. Kent

RFC 4304
Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP) S. Kent

RFC 4307
Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2) J. Schiller

RFC 4308
Cryptographic Suites for IPsec P. Hoffman

RFC 4434
The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol P. Hoffman

RFC 4443
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering

RFC 4552
Authentication/Confidentiality for OSPFv3 M. Gupta, N. Melam

RFC 4678
Server/Application State Protocol v1 A. Bivens

RFC 4753
ECP Groups for IKE and IKEv2 D. Fu, J. Solinas

RFC 4754
IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA) D. Fu, J. Solinas

RFC 4809
Requirements for an IPsec Certificate Management Profile C. Bonatti, Ed., S. Turner, Ed., G. Lebovitz, Ed.

RFC 4835
Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) V. Manral

RFC 4862
IPv6 Stateless Address Autoconfiguration S. Thomson, T. Narten, T. Jinmei

RFC 4868
Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec S. Kelly, S. Frankel

RFC 4869
Suite B Cryptographic Suites for IPsec L. Law, J. Solinas

RFC 4941
Privacy Extensions for Stateless Address Autoconfiguration in IPv6 T. Narten, R. Draves, S. Krishnan

RFC 4945
The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX B. Korver

RFC 5014
IPv6 Socket API for Source Address Selection E. Nordmark, S. Chakrabarti, J. Laganier

RFC 5095
Deprecation of Type 0 Routing Headers in IPv6 J. Abley, P. Savola, G. Neville-Neil

RFC 5175
IPv6 Router Advertisement Flags Option B. Haberman, Ed., R. Hinden

RFC 5282
Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol D. Black, D. McGrew

RFC 5996
Internet Key Exchange Protocol Version 2 (IKEv2) C. Kaufman, P. Hoffman, Y. Nir, P. Eronen

Internet drafts

Internet drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Other groups can also distribute working documents as Internet drafts. You can see Internet drafts at http://www.ietf.org/ID.html.

Appendix B. Architectural specifications

This appendix lists documents that provide architectural specifications for the SNA Protocol.

The APPN Implementers' Workshop (AIW) architecture documentation includes the following architectural specifications for SNA APPN and HPR:

- APPN Architecture Reference (SG30-3422-04)
- APPN Branch Extender Architecture Reference Version 1.1
- APPN Dependent LU Requester Architecture Reference Version 1.5
- APPN Extended Border Node Architecture Reference Version 1.0
- APPN High Performance Routing Architecture Reference Version 4.0
- SNA Formats (GA27-3136-20)
- SNA Technical Overview (GC30-3073-04)

For more information, see the AIW documentation page at http://www.ibm.com/support/docview.wss?rs=852&uid=swg27017843.

The following RFC also contains SNA architectural specifications:

- RFC 2353 *APPN/HPR in IP Networks APPN Implementers' Workshop Closed Pages Document*

RFCs can be obtained from:

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

Many RFCs are available online. Hardcopies of all RFCs are available from the NIC, either individually or by subscription. Online copies are available using FTP from the NIC at http://www.rfc-editor.org/rfc.html.

Use FTP to download the files, using the following format:

```
RFC:RFC-INDEX.TXT
RFC:RFCnnnn.TXT
RFC:RFCnnnn.PS
```

where:

- *nnnn* is the RFC number.
- TXT is the text format.
- PS is the postscript format.

You can also request RFCs through electronic mail, from the automated NIC mail server, by sending a message to `service@nic.ddn.mil` with a subject line of `RFC nnnn` for text versions or a subject line of `RFC nnnn.PS` for PostScript versions. To request a copy of the RFC index, send a message with a subject line of `RFC INDEX`.

For more information, contact nic@nic.ddn.mil.

Appendix C. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you can view the information through the z/OS Internet Library website or IBM Knowledge Center. If you continue to experience problems, send an email to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. See z/OS TSO/E Primer, z/OS TSO/E User's Guide, and z/OS ISPF User's Guide Vol I for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer or 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.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who want 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.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

COPYRIGHT LICENSE:

This information might contain 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.

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.

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 acknowledgment:

```
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. 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.

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.

Copyright © 1991, 1993 The Regents of the University of California.

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 acknowledgment:

   `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.

Copyright © 1990 by the Massachusetts Institute of Technology

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.

Copyright © 1998 by the FundsXpress, INC.

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 FundsXpress not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. FundsXpress makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

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.

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 © 1995-1998 Eric Young (eay@cryptsoft.com)

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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 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 acknowledgment: "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 acknowledgment:

   "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.

Copyright © 1999,2000,2001 Compaq Computer Corporation

Copyright © 1999,2000,2001 Hewlett-Packard Company

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.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: http://www-01.ibm.com/software/support/systemsz/lifecycle/
- For information about currently-supported IBM hardware, contact your IBM representative.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java-based trademarks are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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 xiv.

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.

z/OS Communications Server information

z/OS Communications Server product information is grouped by task in the following tables.

Planning

Title	Number	Description
z/OS Communications Server: New Function Summary	GC27-3664	This document is intended to help you plan for new IP or SNA 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	SC27-3663	This document is a high-level introduction to IPv6. It describes concepts of z/OS Communications Server's support of IPv6, coexistence with IPv4, and migration issues.

Resource definition, configuration, and tuning

Title	Number	Description
z/OS Communications Server: IP Configuration Guide	SC27-3650	This document describes the major concepts involved in understanding and configuring an IP network. Familiarity with the z/OS operating system, IP protocols, z/OS UNIX System Services, and IBM Time Sharing Option (TSO) is recommended. Use this document with the z/OS Communications Server: IP Configuration Reference.

Title	Number	Description
z/OS Communications Server: IP Configuration Reference	SC27-3651	This document presents information for people who want to administer and maintain IP. Use this document with the z/OS Communications Server: IP Configuration Guide. The information in this document includes: • TCP/IP configuration data sets • Configuration statements • Translation tables • Protocol number and port assignments
z/OS Communications Server: SNA Network Implementation Guide	SC27-3672	This document presents the major concepts involved in implementing an SNA network. Use this document with the z/OS Communications Server: SNA Resource Definition Reference.
z/OS Communications Server: SNA Resource Definition Reference	SC27-3675	This document describes each SNA definition statement, start option, and macroinstruction for user tables. It also describes NCP definition statements that affect SNA. Use this document with the z/OS Communications Server: SNA Network Implementation Guide.
z/OS Communications Server: SNA Resource Definition Samples	SC27-3676	This document contains sample definitions to help you implement SNA functions in your networks, and includes sample major node definitions.
z/OS Communications Server: IP Network Print Facility	SC27-3658	This document is for systems programmers and network administrators who need to prepare their network to route SNA, JES2, or JES3 printer output to remote printers using TCP/IP Services.

Operation

Title	Number	Description
z/OS Communications Server: IP User's Guide and Commands	SC27-3662	This document describes how to use TCP/IP applications. It contains requests with which a user can log on to a remote host using Telnet, transfer data sets using FTP, send and receive electronic mail, print on remote printers, and authenticate network users.
z/OS Communications Server: IP System Administrator's Commands	SC27-3661	This document describes the functions and commands helpful in configuring or monitoring your system. It contains system administrator's commands, such as TSO NETSTAT, PING, TRACERTE and their UNIX counterparts. It also includes TSO and MVS commands commonly used during the IP configuration process.
z/OS Communications Server: SNA Operation	SC27-3673	This document serves as a reference for programmers and operators requiring detailed information about specific operator commands.
z/OS Communications Server: Quick Reference	SC27-3665	This document contains essential information about SNA and IP commands.

Customization

Title	Number	Description
z/OS Communications Server: SNA Customization	SC27-3666	This document enables you to customize SNA, and includes the following information: • Communication network management (CNM) routing table • Logon-interpret routine requirements • Logon manager installation-wide exit routine for the CLU search exit • TSO/SNA installation-wide exit routines • SNA installation-wide exit routines

Writing application programs

Title	Number	Description
z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference	SC27-3660	This document describes the syntax and semantics of program source code necessary to write your own application programming interface (API) into TCP/IP. You can use this interface as the communication base for writing your own client or server application. You can also use this document to adapt your existing applications to communicate with each other using sockets over TCP/IP.
z/OS Communications Server: IP CICS Sockets Guide	SC27-3649	This document is for programmers who want to set up, write application programs for, and diagnose problems with the socket interface for CICS using z/OS TCP/IP.
z/OS Communications Server: IP IMS Sockets Guide	SC27-3653	This document is for programmers who want application programs that use the IMS TCP/IP application development services provided by the TCP/IP Services of IBM.
z/OS Communications Server: IP Programmer's Guide and Reference	SC27-3659	This document describes the syntax and semantics of a set of high-level application functions that you can use to program your own applications in a TCP/IP environment. These functions provide support for application facilities, such as user authentication, distributed databases, distributed processing, network management, and device sharing. Familiarity with the z/OS operating system, TCP/IP protocols, and IBM Time Sharing Option (TSO) is recommended.
z/OS Communications Server: SNA Programming	SC27-3674	This document describes how to use SNA macroinstructions to send data to and receive data from (1) a terminal in either the same or a different domain, or (2) another application program in either the same or a different domain.
z/OS Communications Server: SNA Programmer's LU 6.2 Guide	SC27-3669	This document describes how to use the SNA LU 6.2 application programming interface for host application programs. This document applies to programs that use only LU 6.2 sessions or that use LU 6.2 sessions along with other session types. (Only LU 6.2 sessions are covered in this document.)
z/OS Communications Server: SNA Programmer's LU 6.2 Reference	SC27-3670	This document provides reference material for the SNA LU 6.2 programming interface for host application programs.
z/OS Communications Server: CSM Guide	SC27-3647	This document describes how applications use the communications storage manager.

Title	Number	Description
z/OS Communications Server: CMIP Services and Topology Agent Guide	SC27-3646	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	GC27-3652	This document explains how to diagnose TCP/IP problems and how to determine whether a specific problem is in the TCP/IP product code. It explains how to gather information for and describe problems to the IBM Software Support Center.
z/OS Communications Server: ACF/TAP Trace Analysis Handbook	GC27-3645	This document explains how to gather the trace data that is collected and stored in the host processor. It also explains how to use the Advanced Communications Function/Trace Analysis Program (ACF/TAP) service aid to produce reports for analyzing the trace data information.
z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures and z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	GC27-3667 GC27-3668	These documents help you identify an SNA problem, classify it, and collect information about it before you call the IBM Support Center. The information collected includes traces, dumps, and other problem documentation.
z/OS Communications Server: SNA Data Areas Volume 1 and z/OS Communications Server: SNA Data Areas Volume 2	GC31-6852 GC31-6853	These documents describe SNA data areas and can be used to read an SNA dump. They are intended for IBM programming service representatives and customer personnel who are diagnosing problems with SNA.

Messages and codes

Title	Number	Description
z/OS Communications Server: SNA Messages	SC27-3671	This document describes the ELM, IKT, IST, IUT, IVT, and USS messages. Other information in this document includes: • Command and RU types in SNA messages • Node and ID types in SNA messages • Supplemental message-related information
z/OS Communications Server: IP Messages Volume 1 (EZA)	SC27-3654	This volume contains TCP/IP messages beginning with EZA.
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	SC27-3655	This volume contains TCP/IP messages beginning with EZB or EZD.
z/OS Communications Server: IP Messages Volume 3 (EZY)	SC27-3656	This volume contains TCP/IP messages beginning with EZY.
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	SC27-3657	This volume contains TCP/IP messages beginning with EZZ and SNM.
z/OS Communications Server: IP and SNA Codes	SC27-3648	This document describes codes and other information that appear in z/OS Communications Server messages.

Index

Numerics

64-bit common (HVCOMMON) storage 76

A

accessibility 117
address volumes and FTP support 82
agent, VTAM topology 11
APPN
  default COS 12
  default transmission groups 12
APPN route selection trace 47
APPN routing tree corruption 88
AT-TLS enablement for RRSF 73
authorization requirements for real-time TCP/IP network monitoring NMI 83
autonomic quiescing of unresponsive name servers 79
autonomics and CSM constrained conditions 81

B

balancing workloads 65
BIND 9.2.0 function 63
BPX.SUPERUSER authority 68
bypassing host name lookup in otelnetd 85

C

caching DNS responses 63
checksum and segmentation offload 78
Communications Server for z/OS, online information xvi
configuration 43
Configuration Assistant and common configuration of multiple stacks 72
Configuration Assistant and multiple releases 70
Configuration Assistant and password phrases 73
Configuration Assistant and reusable configuration objects 72
Configuration Assistant and RRSF 73
Configuration Assistant and stack IP addresses 70
Configuration Assistant and z/OSMF SAF mode authorization 73
configuration of multiple stacks and Configuration Assistant 72
configuring multiple LPARs 70
connectivity and IEDN 74
connectivity test and Enterprise Extender 87
convergence for sysplex distribution routing when joining a sysplex 80
corruption of routing tree 88
COSAPPN file 12
cryptographic mode 69
CSM constrained conditions for sysplex autonomics 81
CSSMTP and syntax errors 85
CSSMTP extended retry 80

D

data sets 82
data sets, distribution library 4
debugging output 86
disability 117
discovery of stack IP addresses 70
DISPLAY TCPIP,TELNET 84
distribution library data sets 4
DNS responses 63
DNS, online information xvii
DVIPAs 66
dynamically adjust input buffer size 84

E

EE connections and routing information 87
encryption features 2
Enterprise Extender (EE) workloads and traffic 88
Enterprise Extender and HPR packet trace analyzer 88
Enterprise Extender and IDS and traffic 87
Enterprise Extender firewall-friendly connectivity test 87
Ethernet LAN connectivity 74
extended address volumes and FTP support 82
Extended English characters 36
extended retry and CSSMTP 80

F

file processing 85
FIPS 140 cryptographic mode 69
firewall-friendly connectivity test and Enterprise Extender 87
FTP support for extended address volumes 82
FTP support for large-format data sets 82
FTP support for password phrases 67
FTPCHKPWD exit routine 67

H

hierarchical file system) parts for z/OS Communications Server 4
HiperSockets optimization for intraensemble data networks 74
host name lookup in otelnetd 85
HPR packet trace analyzer for Enterprise Extender 88

I

IBM Health Checker 43
IBM Software Support Center, contacting xiii
IBMTGPS file (APPN) 12
ICMP messages 87
IEDN connectivity 74
IKE daemon and superuser requirement 68
IKE version 2 and Sysplex-Wide Security Associations 65
IKED and FIPS mode 69
IKEv2 NAT traversal 64
inbound workload queueing 88
Information APARs xiv
Internet, finding z/OS information online xvi
intraensemble data networks and HiperSockets optimization 74
intrusion detection services 63

intrusion detection services support for Enterprise Extender 87
IP address control 66
IP addresses and Configuration Assistant 70
IP Services 43
IPsec support for FIPS 140 cryptographic mode 69
IPv6 checksum and segmentation offload 78

J

joining a sysplex 80

K

keyboard 117

L

LAN connectivity 74
large-format data sets and FTP supportr 82
license, patent, and copyright information 119
lookup in otelnetd 85
LPARs and configuring 70

M

mainframe
  education xiv
multiple stacks and Configuration Assistant 72
MVS data sets 4
MVS, installing VTAM under 7

N

name servers and system resolver autonomic quiescing 79
NAT traversal 64
network monitoring NMI 83
NMI for retrieving system resolver configuration information 83
NMI, authorization requirements 83

O

O/S data sets used by VTAM 7
OMPROUTE 86
OMPROUTE reports 86
OSA-Express in QDIO mode 88
otelnetd and bypassing host name lookup 85

P

packet trace analyzer for Enterprise Extender 88
packet trace formatting 88
password phrases and FTP support 67
PASSWORDPHRASE option 84
planning checklist 3
Policy Agent and superuser requirement 68
PORTRANGE statement and wildcard support 74
prerequisite information xiv

Q

QDIO IPv6 checksum and segmentation offload 78
QDIO mode and OSA-Express 88
queueing and inbound workload 88
quiescing of unresponsive name servers 79

R

real-time TCP/IP network monitoring NMI 83
removing superuser authority 68
requirements for real-time TCP/IP network monitoring NMI 83
resolver autonomic quiescing of unresponsive name servers 79
resolver configuration information 83
retrieving system resolver configuration information 83
retrying functions 80
RFC (request for comments) 91
  accessing online xvi
RFC 5996 64
router ID 86
RouterID 86
routing and APPN 88
routing information for the EE connection 87
routing tree corruption 88
routing when joining a sysplex 80

S

SA distribution and FIPS mode 69
SAF mode authorization for z/OSMF 73
segmentation offload 78
shortcut keys 117
SNA protocol specifications 115
SNA serviceability enhancements 47
SNMP manager API and routines 86
softcopy information xiv
spool file processing 85
stack IP addresses 70
summary of changes xix
superuser requirement for Policy Agent and IKE daemon 68
support considerations in V1R13 63
support considerations in V2R1 27
sysplex autonomics and CSM constrained conditions 81
sysplex distribution routing when joining a sysplex 80
Sysplex-Wide Security Associations for IKE version 2 65
SYSTCPCN 83
SYSTCPDA 83
SYSTCPOT 84
system resolver autonomic quiescing of unresponsive name servers 79
system resolver configuration information NMI 83

T

TCID statistics 88
TCP/IP
  online information xvi
  protocol specifications 91
TCP/IP legacy device types 43
TCP/IP network monitoring NMI 83
TCP/IP packet trace formatting 88
TCP/IP serviceability 86
TCPIPDS1 76
Technotes xiv

TN3270E server 84
topology agent 11
topology agent, enabling 7
trademark information 127
traffic and EE 88
transmission groups (TG), APPN default 12
TSO/VTAM improvement 36

U

UID(0) authority 68
unresponsive name servers 79

V

VIPARANGE DVIPAs 66
VTAM internal trace (VIT) table 76
VTAM topology agent 11
VTAM topology agent, enabling 7
VTAM, online information xvi

W

wildcard support for the PORTRANGE statement 74
workload balancing 65
workload queueing 88

X

xx 27, 63

Z

z/OS Basic Skills Information Center xiv
z/OS GATEWAY statement 43
z/OS V1R13 Communications Server release summary 63
z/OS V2R1 Communications Server release summary 27
z/OS, documentation library listing 129
z/OSMF SAF mode authorization 73
zSeries, definition of 1
zSystem, definition of 1

Communicating your comments to IBM

If you especially like or dislike anything about this document, you can send us comments electronically by using one of the following methods:

Internet email:
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, and telephone number. Make sure to include the following information in your comment or note:

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

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.

Product Number: 5650-ZOS

Printed in USA

GC27-3664-03