z/OS Communications Server

New Function Summary

Version 1 Release 13

GC31-8771-07

Note:
Before using this information and the product it supports, be sure to read the general information under "Notices" on page 103.

Eighth Edition (September 2011)

This edition applies to Version 1 Release 13 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

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

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

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

Fax (USA and Canada):

1+919-254-1258

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

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

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

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

Contents

Figures

Tables

About this document

The purpose of this document is to describe the exploitation considerations of the new functions for the TCP/IP and SNA components of z/OS® Version 1 Release 13 Communications Server (z/OS Communications Server). It also includes the exploitation considerations of z/OS V1R12 Communications Server.

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

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

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

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

Who should read this document

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

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

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

How this document is organized

This document contains these topics:

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

- Chapter 2, “Roadmap to functions,” on page 21 provides a roadmap of the functional enhancements introduced in z/OS V1R13 Communications Server and z/OS V1R12 Communications Server. Each entry indicates whether enabling or actions are required.
- Chapter 3, “V1R13 new function summary,” on page 25 summarizes the functions and migration considerations of z/OS V1R13 Communications Server.
- Chapter 4, “V1R12 new function summary,” on page 53 summarizes the functions and migration considerations of z/OS V1R12 Communications Server.
- Appendix A, “Related protocol specifications,” on page 81 lists the related protocol specifications for TCP/IP.
- "Architectural specifications" lists documents that provide architectural specifications for the SNA Protocol.
- "Accessibility" describes accessibility features to help users with physical disabilities.
- "Notices" contains notices and trademarks used in this document.
- "Bibliography" contains descriptions of the documents in the z/OS Communications Server library.

How to use this document

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

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

Use the function summary topics to learn about this information:

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

Determining whether a publication is current

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

- At the end of a publication's order number there is a dash followed by two digits, often referred to as the dash level. A publication with a higher dash level is more current than one with a lower dash level. For example, in the publication order number GC28-1747-07, the dash level 07 means that the publication is more current than previous levels, such as 05 or 04.
- If a hardcopy publication and a softcopy publication have the same dash level, it is possible that the softcopy publication is more current than the hardcopy

publication. Check the dates shown in the Summary of Changes. The softcopy publication might have a more recently dated Summary of Changes than the hardcopy publication.

- To compare softcopy publications, you can check the last two characters of the publication's file name (also called the book name). The higher the number, the more recent the publication. Also, next to the publication titles in the CD-ROM booklet and the readme files, there is an asterisk (*) that indicates whether a publication is new or changed.

How to contact IBM service

For immediate assistance, visit this 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, as well as access a variety of diagnosis information.

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

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

If you would like to provide feedback on this publication, see “Communicating your comments to IBM” on page 121.

Conventions and terminology that are used in this document

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

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

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

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

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

For definitions of the terms and abbreviations that are used in this document, you can view the latest IBM terminology at the IBM Terminology 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 113, in the back of this document.

Required information

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

Softcopy information

Softcopy publications are available in the following collections.

Titles	Order Number	Description
z/OS V1R13 and Software Products DVD Collection	SK3T-4271	This collection includes the libraries of z/OS (the element and feature libraries) and the libraries for z/OS software products in both BookManager format and PDF files. This collection combines SK3T-4269 and SK3T-4270.
IBM System z Redbooks Collection	SK3T-7876	The Redbooks® selected for this CD series are taken from the IBM® Redbooks inventory of over 800 books. All the Redbooks that are of interest to the zSeries® platform professional are identified by their authors and are included in this collection. The zSeries subject areas range from e-business application development and enablement to hardware, networking, Linux, solutions, security, parallel sysplex, and many others.

Other documents

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

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

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

Title	Number
DNS and BIND, Fifth Edition, O'Reilly Media, 2006	ISBN 13: 978-0596100575
Routing in the Internet , Second Edition, Christian Huitema (Prentice Hall 1999)	ISBN 13: 978-0130226471
sendmail, Fourth Edition, Bryan Costales, Claus Assmann, George Jansen, and Gregory Shapiro, O'Reilly Media, 2007	ISBN 13: 978-0596510299
SNA Formats	GA27-3136
TCP/IP Illustrated, Volume 1: The Protocols, W. Richard Stevens, Addison-Wesley Professional, 1994	ISBN 13: 978-0201633467
TCP/IP Illustrated, Volume 2: The Implementation, Gary R. Wright and W. Richard Stevens, Addison-Wesley Professional, 1995	ISBN 13: 978-0201633542
TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols, W. Richard Stevens, Addison-Wesley Professional, 1996	ISBN 13: 978-0201634952
TCP/IP Tutorial and Technical Overview	GG24-3376
Understanding LDAP	SG24-4986
z/OS Cryptographic Services System SSL Programming	*SC24-5901*
z/OS Integrated Security Services LDAP Server Administration and Use	*SC24-5923*
z/OS JES2 Initialization and Tuning Guide	*SA22-7532*
z/OS Problem Management	*G325-2564*
z/OS MVS Diagnosis: Reference	*GA22-7588*
z/OS MVS Diagnosis: Tools and Service Aids	*GA22-7589*
z/OS MVS Using the Subsystem Interface	*SA22-7642*
z/OS Program Directory	*GI10-0670*
z/OS UNIX System Services Command Reference	*SA22-7802*
z/OS UNIX System Services Planning	*GA22-7800*
z/OS UNIX System Services Programming: Assembler Callable Services Reference	*SA22-7803*
z/OS UNIX System Services User's Guide	*SA22-7801*
z/OS XL C/C++ Run-Time Library Reference	*SA22-7821*
zEnterprise 196, System z10, System z9 and eServer zSeries OSA-Express Customer's Guide and Reference	*SA22-7935*

Redbooks

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

Title	Number
IBM z/OS V1R12 Communications Server TCP/IP Implementation, Volume 1: Base Functions, Connectivity, and Routing	SG24-7896
IBM z/OS V1R12 Communications Server TCP/IP Implementation, Volume 2: Standard Applications	SG24-7897

Title	Number
IBM z/OS V1R12 Communications Server TCP/IP Implementation, Volume 3: High Availability, Scalability, and Performance	SG24-7898
IBM z/OS V1R12 Communications Server TCP/IP Implementation, Volume 4: Security and Policy-Based Networking	SG24-7899
IBM Communication Controller Migration Guide	SG24-6298
IP Network Design Guide	SG24-2580
Managing OS/390® TCP/IP with SNMP	SG24-5866
Migrating Subarea Networks to an IP Infrastructure Using Enterprise Extender	SG24-5957
SecureWay™ Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements	SG24–5631
SNA and TCP/IP Integration	SG24-5291
TCP/IP in a Sysplex	SG24-5235
TCP/IP Tutorial and Technical Overview	GG24-3376
Threadsafe Considerations for CICS	SG24-6351

Where to find related information on the Internet

z/OS

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

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

z/OS Internet Library

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

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

IBM Communications Server product

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

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

IBM Communications Server product support

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

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

IBM Communications Server performance information

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

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

IBM Systems Center publications

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

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

IBM Systems Center flashes

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

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

RFCs

Search for and view Request for Comments documents in this section of the Internet Engineering Task Force 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 in any manner 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 system programmer.

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

- Provide basic education and information about z/OS without charge

- Shorten the time it takes for people to become productive on the mainframe
- Make it easier for new people to learn z/OS

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

How to send your comments

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

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

Summary of changes

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

Changes made in z/OS Communications Server Version 1 Release 13

This document contains information previously presented in *z/OS Communications Server: New Function Summary*, GC31-8771-06, which supports z/OS Version 1 Release 12.

New information:

Chapter 3, "V1R13 new function summary," on page 25 includes descriptions for the new functions and enhancements introduced in this release and explains how to use them. Entries for the new functions and enhancements are added to Chapter 2, "Roadmap to functions," on page 21.

Deleted information:

The release summary chapters for z/OS V1R11 are deleted and the V1R11 entries are deleted from Chapter 2, "Roadmap to functions," on page 21. You can still access the old release summary documentation at this web site: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/.

Changes made in z/OS Communications Server Version 1 Release 12

This document contains information previously presented in *z/OS Communications Server: New Function Summary*, GC31-8771-05, which supports z/OS Version 1 Release 11.

New information:

Chapter 4, "V1R12 new function summary," on page 53 includes descriptions for the new functions and enhancements introduced in this release and explains how to use them. Entries for the new functions and enhancements are added to Chapter 2, "Roadmap to functions," on page 21.

Deleted information:

The release summary chapters for z/OS V1R10 are deleted and the V1R10 entries are deleted from Chapter 2, "Roadmap to functions," on page 21. You can still access the old release summary documentation at this web site: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/.

Chapter 1. Planning to use new functions

These topics help you plan to use new functions:

Introduction to z/OS Communications Server

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

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

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

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

- The IBM zEnterprise™TM System (zEnterprise) product line consists of 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), 890 (z890), 900 (z900) and 800 (z800).
- The IBM System 390 (S/390®) product line includes the IBM S/390 Parallel Enterprise Server Generation 5 (G5) and Generation 6 (G6), and the IBM S/390 Multiprise 3000 Enterprise Server.

The z196, z114, z10 EC, z10 BC, z9 EC (formerly z9-109), z9 BC, z990, z890, z900, and z800 servers are also known as z/Architecture® servers. z/OS V1R13 Communications Server runs only in z/Architecture mode on z/Architecture servers. The G5, G6, and Multiprise 3000 servers are not supported for z/OS V1R13 Communications Server.

Determining which documents to use when migrating

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

Table 1. Comparing documents used in migration

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

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

IP encryption features

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

The encryption features include these capabilities:

Level 1
This level of encryption is included in the base of z/OS V1R13 Communications Server.

Level 2
This level of encryption is included in the base of z/OS V1R13 Communications Server and offers IP security protocol (IPSec) DES and SNMPv3 56-bit DES.

Level 3

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

Planning checklist

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

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

__ 2. Understand that z/OS V1R13 Communications Server is a base element of z/OS. Use the appropriate documents as you plan, migrate, and install:

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

For information about installation, see these documents:

- *z/OS Program Directory*
- Preventative Service Planning (PSP) bucket (available by using IBMLINK)
- Softcopy Installation Memo (for Bookmanager publications)
- *ServerPac: Installing Your Order*, if you use the ServerPac method to install z/OS

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

__ 3. Develop your education plan:
- Evaluate the z/OS V1R13 Communications Server features and enhancements by reading the new function summary topics in this document. Plan which new functions will be incorporated into your system.

__ 4. Review and apply the Program Temporary Fixes (PTFs), including Recommended Service Upgrades (RSUs), for the current-minus-3 month plus all hipers and PEs. The PTFs are available monthly through the period for which the release is current and can be obtained by using IBMLINK. RSU integration testing for a release will be performed for five quarters after the general availability date for that release.

__ 5. Get acquainted with the helpful information found at z/OS Communications Server Support.

__ 6. In writing a test plan for z/OS, include test cases for these items:
- TCP/IP applications
- Key or critical SNA applications and Original Equipment Manufacturer (OEM) software products.
- User-written applications such as: Customer Information Control System (CICS®) sockets, Information Management System (IMS™) sockets, REXX sockets, Sockets Extended, UNIX System Services sockets, and Macro Sockets
- Operator commands
- Your terminal and printer types

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

__ 8. Install z/OS Communications Server with the other elements and features of z/OS. IBM has defined the appropriate product enablement settings in the IFAPRD00 member of SYS1.IBM.PARMLIB. For information about dynamic enablement, see *z/OS Planning for Installation*.

__ 9. Complete post-installation activities:
- Use *z/OS Communications Server: IP Configuration Guide* to customize your TCP/IP system.
- Use the following to customize your SNA system:
  - *z/OS Communications Server: SNA Customization*
  - *z/OS Communications Server: SNA Network Implementation Guide*
  - *z/OS Communications Server: SNA Resource Definition Reference*
- Use *z/OS Migration* to determine migration actions.
- Reinstall user exits.
- Reinstall user modifications.
- Update operating procedures and automation routines.
- Activate new functions.

__ 10. Complete functional and stress tests.

TCP/IP packaging process

As a result of the installation process for z/OS V1R13 Communications Server, the product is installed in both traditional MVS data sets and in files in the z/OS UNIX HFS. For details on changes in the MVS data sets, see "MVS data sets." For details on requirements for HFS files, see "File system files" on page 7.

MVS data sets

Table 2 lists the distribution library data sets required by z/OS V1R13 Communications Server.

Table 2. Distribution library data sets

Data set	Description
AEZADBR1	Database Request Module (DBRM) members
AHELP	TSO help files
AEZAMAC1	Assembler macros
AEZAMAC2	C header files
AEZAMAC3	Pascal include files
AEZAMODS	Distribution library for base link-edit modules
AEZARNT1	Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS
AEZARNT2	Reentrant object module for SEZAXAWL
AEZARNT3	Reentrant object module for SEZAXMLB
AEZAROE2	Reentrant object module for SEZAXAWL (z/OS UNIX support)
AEZAROE3	Reentrant object module for SEZAXMLB (z/OS UNIX support)
AEZARNT4	Reentrant object modules for RPC
AEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)

Table 2. Distribution library data sets (continued)

Data set	Description
AEZASMP1	Sample source programs, catalog procedures, CLIST, and installation jobs
AEZAXLTD	Translated default tables
AEZAXLTK	Translated Kanji, Hangeul, and Traditional Chinese DBCS tables and codefiles
AEZAXLT1	Translation table SBCS source and DBCS source for Hangeul and Traditional Chinese
AEZAXLT2	TELNET client translation tables
AEZAXLT3	Kanji DBCS translation table source
ABLSCLI0	clists, execs, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSMSG0	messages, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSPNL0	panels, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSTBL0	tables, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables

Table 3 lists the target library data sets required by z/OS V1R13 Communications Server.

Table 3. Target library data sets

Data set	Description
SEZACMAC	Client Pascal macros, C headers, and assembler macros
SEZACMTX	Load library for linking user modules and programs
SEZADBCX	Source for the Kanji, Hangeul, and Traditional Chinese DBCS translation tables
SEZADBRM	DBRM members
SEZADPIL	SNMP Distributed Programming Interface library
SEZADSIL	SNMP command processor and SNMPIUCV subtask for the NetView® program, and the SQESERV module for the SNMP query engine
SEZADSIM	SNMP messages for the NetView program
SEZADSIP	SNMPIUCV initialization parameters for the NetView program
SEZAEXEC	CLISTs and REXX programs
SEZAINST	Installation samples and related members
SEZALIBN	NCS library system library
SEZALOAD	Executable load modules for concatenation to LINKLIB
SEZALNK2	LB@ADMIN for the NCS administrator
SEZALPA	Executable load modules for concatenation to LPALST
SEZAMENU	ISPF messages
SEZANCLS	NetView SNMP CLISTs
SEZANMAC	C headers and assembler macros for z/OS UNIX and TCP/IP Services APIs
SEZANPNL	NetView SNMP panels

Table 3. Target library data sets (continued)

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

Table 4 lists the shared distribution and target library data sets required by z/OS V1R13 Communications Server.

Table 4. Shared distribution and target library data sets

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

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

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

File system files

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

Defining SNA data sets

This section describes z/OS data sets that you need to define or modify for z/OS V1R13 Communications Server. Table 5 shows the z/OS data sets that contain information for z/OS V1R13 Communications Server, and Table 6 on page 9 shows the z/OS data sets that contain information for both VTAM and NCP.

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

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

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

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

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

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

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

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

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

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

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

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

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

Data sets containing information for z/OS V1R13 Communications Server

This section describes data sets that contain information for z/OS V1R13 Communications Server.

SYS1.SISTCLIB

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

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

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

   ```
   //SISTCLIB DD   DSN=SYS1.SISTCLIB,DISP=SHR
   ```
3. Define SYS1.SISTCLIB as an authorized library (a library listed in the currently used IEAAPF*xx*).

SYS1.SISTCMIP

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

The LRECL for this file is 80.

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

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

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

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

SYS1.SISTASN1

The LRECL for this file is 1024.

SYS1.VTAMLST

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

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

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

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

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

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

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

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

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

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

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

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

Guidelines:

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

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

SYS1.VTAMLIB

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

SYS1.VTAMLIB is used to store these user tables:

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

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

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

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

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

Parmlib member for Communication Storage Manager (CSM)

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

The parameter member IVTPRM00 can be found in:

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

IVTPRM00 has this format:

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

       FIXED MAX(maxfixK|M)

       ECSA MAX(maxecsaK|M)

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

Rules:

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

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

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

This describe the variable fields in the CSM parmlib member:

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

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

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

K Denotes size in kilobytes

M Denotes size in megabytes.

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

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

ECSA Buffers are allocated from ECSA storage.

DSPACE
Buffers are allocated from data space storage.

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

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

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

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

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

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

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

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

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

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

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

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

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

APPN checkpointing data sets

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

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

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

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

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

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

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

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

SYS1.TRSDB is required for checkpointing the network topology database. The information in this data set is used to initialize the network topology database whenever z/OS V1R13 Communications Server is restarted. The network topology database is written to this file whenever a **MODIFY CHKPT TYPE=TOPO** or **TYPE=ALL, HALT**, or **HALT QUICK** command is issued.

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

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

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

- Specify these DCB subparameters for SYS1.DSDBCTRL:

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

Notes:

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

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

Configuration restart data sets

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

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

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

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

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

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

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

Dynamic configuration data sets for channel-attached devices

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

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

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

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

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

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

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

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

First Failure Support Technology

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

NODELST data set

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

To define a NODELST data set, perform these steps:

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

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

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

You can use defaults for all other data characteristics.

Data sets containing information for NCP

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

NCP load library

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

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

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

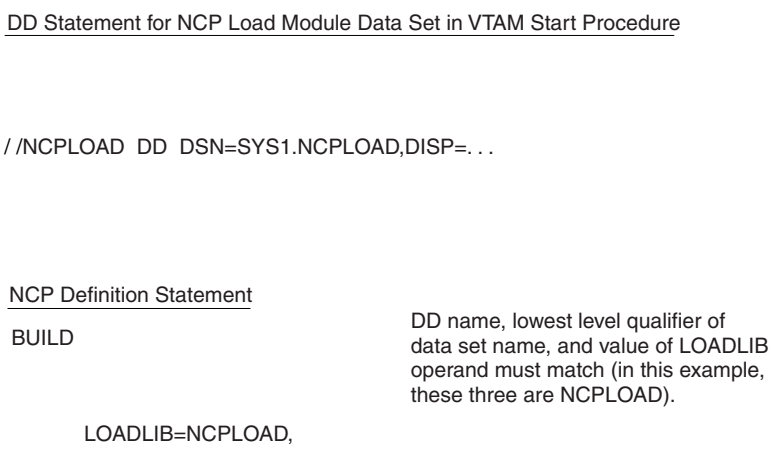

Figure 1. Correlation between DD statement and NCP definition statement

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

SYS1.SSPLIB

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

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

NCP dump

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

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

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

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

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

Loader channel I/O trace

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

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

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

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

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

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

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

Chapter 2. Roadmap to functions

This topic includes a roadmap table to all of the functions and enhancements that were introduced in z/OS V1R13 Communications Server and z/OS V1R12 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 V1R13 Communications Server	
"Expanded intrusion detection services" on page 25	Yes
"Network address translation traversal support for IKE version 2" on page 26	Yes
"Sysplex-Wide Security Associations for IKE version 2" on page 27	Yes
"Improved security granularity for VIPARANGE DVIPAs" on page 28	Yes
"FTP support for password phrases" on page 29	Optional
"Removed superuser requirement for Policy Agent and IKE daemon" on page 30	Yes
"Enhanced IPsec support for FIPS 140 cryptographic mode" on page 31	Yes
"Configuration Assistant management of multiple z/OS Communications Server releases" on page 32	Yes
"Configuration Assistant discovery of stack IP addresses" on page 32	Yes
"Configuration Assistant common configuration of multiple stacks" on page 34	Yes
"Configuration Assistant enhancements" on page 35	Yes
"Wildcard support for the PORTRANGE statement" on page 36	Yes
"HiperSockets optimization for intraensemble data networks" on page 36	Yes
"Support for additional VLANs for an OSA-Express QDIO port" on page 37	Yes
"Increased CTRACE and VIT capacity" on page 38	Optional
"OSA-Express4S QDIO IPv6 checksum and segmentation offload" on page 40	Yes
"System resolver autonomic quiescing of unresponsive name servers" on page 41	Yes
"Improved convergence for sysplex distribution routing when joining a sysplex" on page 42	No
"CSSMTP extended retry" on page 42	Yes
"Monitor CSM constrained conditions for sysplex autonomics" on page 43	Optional
"Enhanced FTP support for extended address volumes" on page 44	Yes
"FTP support for large-format data sets" on page 44	Yes
"NMI for retrieving system resolver configuration information" on page 45	Yes
"Simplified authorization requirements for real-time TCP/IP network monitoring NMI" on page 45	Yes
"Enhancements to the TN3270E server" on page 46	Yes
"CSSMTP enhancements" on page 47	Yes
"Support for bypassing host name lookup in otelnetd" on page 47	Yes
"TCP/IP serviceability enhancements" on page 48	Yes

Table 8. Roadmap to functions (continued)

Functional enhancement	Exploitation actions
"Intrusion detection services support for Enterprise Extender" on page 49	Yes
"Enterprise Extender firewall-friendly connectivity test" on page 49	Yes
"HPR packet trace analyzer for Enterprise Extender" on page 50	Yes
"Improved APPN routing resilience" on page 50	No
"Performance improvements for Enterprise Extender traffic" on page 50	Yes
Enhancements introduced in z/OS V1R12 Communications Server	
"Enhancements to IPv6 router advertisement" on page 53	Yes
"Configurable default address selection policy table" on page 54	Yes
"Socket API support for source address selection" on page 54	Yes
"Resolver support for IPv6 connections to DNS name servers" on page 55	Yes
"Performance improvements for sysplex distributor connection routing" on page 56	Yes
"Performance improvements for streaming bulk data" on page 58	Yes
"z/OS Communications Server in an ensemble" on page 59	Yes
"Extend sysplex distributor support for DataPower for IPv6" on page 61	Yes
"Improvements to AT-TLS performance" on page 61	No
"Sysplex distributor support for hot-standby server" on page 62	Yes
"Common storage reduction for TN3270E server" on page 62	Yes
"Performance improvements for fast local sockets" on page 63	No
"Improved resolver reaction to unresponsive DNS name servers" on page 63	No
"Sysplex autonomics monitoring TCP/IP abends" on page 63	No
"IKE version 2 support" on page 64	Yes
"IPSec support for certificate trust chains and certificate revocation lists" on page 65	Yes
"IPSec support for cryptographic currency" on page 66	Yes
"IPSec support for FIPS 140 cryptographic mode" on page 67	Yes
"Trusted TCP connections" on page 68	Yes
"Digital certificate access server (DCAS) MODIFY command for debug level" on page 69	Yes
"Enhancements to the TN3270E server" on page 70	Yes
"IBM Health Checker for z/OS OMPROUTE checks" on page 70	Yes
"Command to drop all connections for a server" on page 71	Yes
"Control joining the sysplex XCF group" on page 71	Yes
"Extension of the retry time limit for CSSMTP" on page 72	Yes
"Enterprise Extender connection health verification" on page 72	Yes
"Multipath control for Enterprise Extender" on page 73	Yes
"Improved recovery from RTP pipe stalls" on page 73	No
"Enhancements to topology database diagnostics" on page 74	Yes
"Performance improvement to TCP/IP callable NMI (EZBNMIFR) GetConnectionDetail request" on page 74	No
"Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics" on page 75	Yes
"SMF event records for sysplex events" on page 75	Yes

Table 8. Roadmap to functions (continued)

Functional enhancement	Exploitation actions
"Management data for CSSMTP" on page 76	Yes
"Data trace records for socket data flow start and end" on page 77	Yes
"Enhancements to the TN3270E server - session manager sends CV64" on page 78	Yes
"Operator command to query and display OSA information" on page 78	Yes
"Packet trace filtering for encapsulated packets" on page 79	Yes
"Verify Netstat message catalog synchronization" on page 79	Yes
"Enhancements to the TCP/IP storage display" on page 80	Yes
"Enhancements to SNMP manager API" on page 80	Yes

Chapter 3. 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 21 for a complete list of the functional enhancements.

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

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

Support considerations in 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 26
- "Sysplex-Wide Security Associations for IKE version 2" on page 27
- "Improved security granularity for VIPARANGE DVIPAs" on page 28
- "FTP support for password phrases" on page 29
- "Removed superuser requirement for Policy Agent and IKE daemon" on page 30
- "Enhanced IPsec support for FIPS 140 cryptographic mode" on page 31
- "Intrusion detection services support for Enterprise Extender" on page 49

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.

Restrictions: 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 49 for information about the IDS support for Enterprise Extender (EE).

Using the expanded intrusion detection services

If you want to use the expanded IDS, perform the appropriate tasks in Table 9.

Table 9. Expanded intrusion detection services

Task	Reference
Enable new IDS policies using the 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 81.

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

If you want to use the NATT support for IKE version 2, perform the appropriate tasks in Table 10.

Table 10. 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 the 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; see "IKE version 2 support" on page 64. 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 are 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

If you want to use SWSA for IKEv2, perform the appropriate tasks in Table 11.

Table 11. 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

If you want to use the improved security granularity for VIPARANGE DVIPAs, perform the appropriate tasks in Table 12.

Table 12. 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 12. 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

If you want to use the FTP support for password phrases, perform the appropriate tasks in Table 13.

Table 13. 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 14 to remove the superuser authority from the servers.

Table 14. 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 14. 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 15.

Table 15. 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 34
- "Configuration Assistant enhancements" on page 35
- "Wildcard support for the PORTRANGE statement" on page 36

Configuration Assistant management of multiple z/OS Communications Server releases

In z/OS V1R13 Communications Server, you can use the 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

If you want to use the Configuration Assistant to manage multiple z/OS Communications Server releases, perform the appropriate tasks in Table 16.

Table 16. 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

If you want to use the Configuration Assistant discovery of stack IP addresses, perform the appropriate tasks in Table 17.

Table 17. 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 17. 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 the 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 17. 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. Reusable rules allow you to 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

If you want to use the Configuration Assistant to configure multiple stacks, perform the appropriate tasks in Table 18 on page 35.

Table 18. 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

If you want to use the Configuration Assistant enhancements, perform the appropriate tasks in Table 19 on page 36.

Table 19. 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

If you want to use the wildcard support for the PORTRANGE statement, perform the task in Table 20.

Table 20. 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 37

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 (see "z/OS Communications Server in an ensemble" on page 59 for more information). 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

If you want to use the HiperSockets optimization for intraensemble data networks, perform the appropriate tasks in Table 21.

Table 21. 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).	*z/OS HCD Reference Summary*
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

If you want to use the support for additional VLANs for an OSA-Express QDIO port, perform the appropriate tasks in Table 22.

Table 22. 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 40

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 23 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 23. 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 23. 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

If you want to use the OSA-Express4S QDIO IPv6 checksum and segmentation offload, perform the appropriate tasks in Table 24.

Table 24. 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 24. 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 42
- "CSSMTP extended retry" on page 42
- "Monitor CSM constrained conditions for sysplex autonomics" on page 43

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.

Restrictions: 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

If you want to use the system resolver autonomic quiescing of unresponsive name servers, perform the appropriate tasks in Table 25 on page 42.

Table 25. 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

If you want to use the CSSMTP extended retry, perform the appropriate tasks in Table 26.

Table 26. 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

If you want to use the enhanced monitoring of CSM usage for sysplex autonomics, perform the task in Table 27.

Table 27. 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

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

If you want to use the enhanced FTP support for extended address volumes, perform the appropriate tasks in Table 28.

Table 28. Enhanced FTP support for extended address volumes

Task	Reference
Learn about extended address volumes and EAS-eligible data sets.	Using the z/OS V1R12 extended address volumes enhancements in *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

If you want to use FTP transfer to and from physical sequential large format data sets, perform the appropriate tasks in Table 29 on page 45. 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 29. 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. If you want to use this NMI, perform the task in Table 30.

Table 30. 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

If you want to use the simplified authorization requirements for real-time TCP/IP network monitoring NMI, perform the task in Table 31.

Table 31. 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

If you want to use the new DISPLAY TCPIP,TELNET command or the PASSWORDPHRASE option, perform the tasks in Table 32. There are no tasks to enable the support for the dynamically adjusted input buffer; it is automatically enabled.

Table 32. 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

If you want to use the CSSMTP enhancements, perform the tasks in Table 33

Table 33. 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

If you want to use the support for bypassing host name lookup in otelnetd, perform the task in Table 34 on page 48

Table 34. 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

If you want to use the TCP/IP serviceability enhancements, perform the appropriate tasks in Table 35.

Table 35. 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

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

If you want to use the IDS support for EE, perform the appropriate tasks in Table 36.

Table 36. 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

If you want to use the EE firewall-friendly connectivity test, perform the appropriate tasks in Table 37.

Table 37. 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

If you want to use the HPR packet trace analyzer for EE, perform the task in Table 38.

Table 38. 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.

Restriction: 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.

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

If you want to use the performance improvements for EE traffic, perform the appropriate tasks in Table 39.

Table 39. 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*
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*

Chapter 4. V1R12 new function summary

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

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

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

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

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

Application integration, data consolidation, and standards

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

- "Enhancements to IPv6 router advertisement"
- "Configurable default address selection policy table" on page 54
- "Socket API support for source address selection" on page 54
- "Resolver support for IPv6 connections to DNS name servers" on page 55

Enhancements to IPv6 router advertisement

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

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

This function is automatically enabled. Use the tasks in Table 40 to display IPv6 routes.

Table 40. Enhancements to IPV6 router advertisement

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

Configurable default address selection policy table

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

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

Using the configurable default address selection policy table

If you want to use the configurable default address selection policy table, perform the appropriate tasks in Table 41.

Table 41. Configurable default address selection policy table

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

Socket API support for source address selection

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

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

Restrictions:

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

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

Using the socket API support for source address selection

If you want to use the socket API support for source address selection, perform the appropriate tasks in Table 42.

Table 42. Socket API support for source address selection

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

Resolver support for IPv6 connections to DNS name servers

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

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

Using the resolver support for IPv6 connections to DNS name servers

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

Table 43. Resolver support for IPv6 connections to DNS name servers

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

Table 43. Resolver support for IPv6 connections to DNS name servers (continued)

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

Scalability, performance, constraint relief, and accelerators

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

Performance improvements for sysplex distributor connection routing

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

Restrictions: The following restrictions apply:

- This function is not supported when z/OS V1R12 Communications Server is running as a z/OS guest on z/VM that is using simulated (virtual) devices such as Virtual Switch (VSWITCH) or guest LAN.
- When traffic is sent over an OSA port that is shared by the receiving TCP/IP stack, QDIO inbound workload queueing does not apply for the traffic that uses an indirect route (where the next hop and destination IP address are different). OSA places such traffic on the primary input queue. If the traffic taking the shared OSA path uses a direct route (where the next hop and destination IP address are the same), QDIO inbound workload queueing applies.

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

Dependencies:

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

Coexistence consideration: Using this function also enables the performance improvements for streaming bulk data; see "Performance improvements for streaming bulk data" on page 58.

Using the performance improvements for sysplex distributor connection routing

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

Table 44. Performance improvements for sysplex distributor connection routing

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

Table 44. Performance improvements for sysplex distributor connection routing (continued)

Task	Reference
Determine whether specific IP traffic is using QDIO inbound workload queueing from a packet trace or OSAENTA trace.	Formatting packet traces using IPCS in *z/OS Communications Server: IP Diagnosis Guide*

Performance improvements for streaming bulk data

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

Restrictions: The following restrictions apply:

- This function is not supported when z/OS V1R12 Communications Server is running as a z/OS guest on z/VM that is using simulated (virtual) devices such as Virtual Switch (VSWITCH) or guest LAN.
- When traffic is sent over an OSA port that is shared by the receiving TCP/IP stack, QDIO inbound workload queueing does not apply for the traffic that uses an indirect route (where the next hop and destination IP address are different). OSA places such traffic on the primary input queue. If the traffic taking the shared OSA path uses a direct route (where the next hop and destination IP address are the same), QDIO inbound workload queueing applies.

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

Dependencies:

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

Coexistence consideration: Using this function also enables the performance improvements for sysplex distributor connection routing; see "Performance improvements for sysplex distributor connection routing" on page 56.

Using the performance improvements for streaming bulk data

If you want to use this function, perform the appropriate tasks in Table 45 on page 59.

Table 45. Performance improvements for streaming bulk data

Task	Reference
Enable inbound workload queueing for a specific QDIO interface by specifying INBPERF DYNAMIC WORKLOADQ on the IPAQENET or IPAQENET6 INTERFACE statement (if necessary). For IPv4 QDIO interfaces that are defined by using the DEVICE, LINK, and HOME statements, you must first convert the statement definitions to use an IPAQENET INTERFACE statement.	• INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces statements in *z/OS Communications Server: IP Configuration Reference* • Steps to convert from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement in *z/OS Communications Server: IP Configuration Guide*
Display whether inbound workload queueing is in effect for the QDIO interface by issuing the Netstat DEvlinks/-d command.	Netstat DEvlinks/-d report in *z/OS Communications Server: IP System Administrator's Commands*
Display whether inbound workload queueing is in effect for the QDIO interface (and display the relationship between workload queueing functions and queue IDs for that interface) by issuing the DISPLAY NET,ID=trle command or the DISPLAY NET,TRL,TRLE=trle command.	DISPLAY ID command and DISPLAY TRL command in *z/OS Communications Server: SNA Operation*
Monitor whether inbound traffic is using inbound workload queueing by initiating VTAM tuning statistics for the QDIO interface.	MODIFY TNSTAT command in *z/OS Communications Server: SNA Operation*
Determine whether a QDIO inbound workload queueing bulk data queue is being used for a TCP connection. Perform one of the following actions: • Invoke the Netstat ALL/-A command. • Update your network management application to use the information returned by the GetConnectionDetail callable NMI.	• Netstat ALL/-A report in *z/OS Communications Server: IP System Administrator's Commands* • GetConnectionDetail request (an EZBNMIFR request) in *z/OS Communications Server: IP Programmer's Guide and Reference*
Display the total number of TCP segments processed on all bulk data queues by invoking the Netstat STATS/-S command or updating your network management application to invoke the GetGlobalStats callable NMI.	Netstat ALL/-A report in *z/OS Communications Server: IP System Administrator's Commands*
Determine whether specific IP traffic is using QDIO inbound workload queueing from a packet trace or OSAENTA trace.	Formatting packet traces using IPCS in *z/OS Communications Server: IP Diagnosis Guide*

z/OS Communications Server in an ensemble

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

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

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

Restrictions:

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

Dependencies:

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

Using z/OS Communications Server in an ensemble

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

Table 46. z/OS Communications Server in an ensemble

Task	Reference
Allow z/OS Communications Server to have connectivity to the intranode management network and to the intraensemble data network by specifying ENSEMBLE=YES as a VTAM start option.	ENSEMBLE start option in *z/OS Communications Server: SNA Resource Definition Reference*
Allow a host management application to have access to the intranode management network by defining the SERVAUTH profile EZB.OSM.*sysname.tcpname* and by authorizing the host management application to the EZB.OSM.*sysname.tcpname* resource.	TCP/IP in an ensemble in *z/OS Communications Server: IP Configuration Guide*
For any TCP/IP stack needing access to the intraensemble data network, define INTERFACE statements as required for each OSA-Express3 CHPID that is configured with a CHPID type of OSX through which access is needed. Define INTERFACE statements for each IP version to be used (IPv4, IPv6, or both). If you require access over multiple VLANs, define an INTERFACE statement for each VLAN that is accessed over the OSA-Express3 interface.	• INTERFACE — IPAQENET OSA-Express QDIO interfaces and INTERFACE — IPAQENET6 OSA-Express QDIO interfaces statements in *z/OS Communications Server: IP Configuration Reference* • TCP/IP in an ensemble in *z/OS Communications Server: IP Configuration Guide*

Table 46. z/OS Communications Server in an ensemble (continued)

Task	Reference
Display information for OSA-Express3 interfaces that are providing connectivity to the internal networks by issuing the Netstat/DEvlinks/-d command, DISPLAY NET,ID=trle, or the DISPLAY NET,TRL,TRLE= command.	• Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands* • DISPLAY ID command and DISPLAY TRL command in *z/OS Communications Server: SNA Operation*
If IPSec is configured and you want a security class for IP filtering for intranode management network interfaces, specify OSMSECCLASS on the IPCONFIG6 statement.	• IPCONFIG6 statement in *z/OS Communications Server: IP Configuration Reference* • TCP/IP in an ensemble in *z/OS Communications Server: IP Configuration Guide*
Display the security class for IP filtering for intranode management network interfaces.	Netstat CONFIG/-f report in *z/OS Communications Server: IP System Administrator's Commands*

Extend sysplex distributor support for DataPower for IPv6

z/OS V1R12 Communications Server introduces sysplex distribution of IPv6 connections to non-z/OS targets, which is similar to the sysplex distribution of IPv4 connections to non-z/OS targets that was introduced in z/OS V1R11 Communications Server.

An IBM WebSphere® DataPower® appliance is currently the only non-z/OS target that supports sysplex distributor load balancing. DataPower appliances are often used as a front-end processing tier for z/OS applications, which provides more efficient handling of web services for a second tier of z/OS applications. When the DataPower tier completes a request, DataPower can route the request to a tier 2 sysplex distributor, which can load balance the request to the second tier of z/OS applications.

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

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

Extending sysplex distributor support for DataPower for IPv6

If you want to use this function, perform the task in Table 47.

Table 47. Extend sysplex distributor support for DataPower for IPv6

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

Improvements to AT-TLS performance

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

Sysplex distributor support for hot-standby server

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

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

Using the sysplex distributor support for hot-standby server

If you want to use this function, perform the appropriate tasks in Table 48.

Table 48. Sysplex distributor support for hot-standby server

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

Common storage reduction for TN3270E server

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

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

Using common storage reduction for TN3270E server

If you want to use this function, perform the appropriate tasks in Table 49.

Table 49. Common storage reduction for TN3270E server

Task	Reference
Specify the SHAREACB statement in the TELNETGLOBALS section of the Telnet profile to enable ACB sharing.	• Reducing demand for ECSA storage in *z/OS Communications Server: IP Configuration Guide* • SHAREACB statement in *z/OS Communications Server: IP Configuration Reference*
Replace any predefined (static) APPL definition statements that are used to represent Telnet LUs with corresponding model application program definition statements.	Reducing demand for ECSA storage in *z/OS Communications Server: IP Configuration Guide*

Table 49. Common storage reduction for TN3270E server (continued)

Task	Reference
Verify that ACB sharing is correctly implemented by issuing the DISPLAY Telnet PROFILE command.	DISPLAY Telnet PROFILE command in *z/OS Communications Server: IP System Administrator's Commands*

Performance improvements for fast local sockets

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

Improved resolver reaction to unresponsive DNS name servers

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

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

Using the improved resolver reaction to unresponsive DNS name servers

The system default is 25% of resolver queries sent to the name server. There are no tasks to enable this function; it is automatically enabled. You can optionally perform the task in Table 50.

Table 50. Improved resolver reaction to unresponsive DNS name servers

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

Sysplex autonomics monitoring TCP/IP abends

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

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

Security

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

- "IKE version 2 support"
- "IPSec support for certificate trust chains and certificate revocation lists" on page 65
- "IPSec support for cryptographic currency" on page 66
- "IPSec support for FIPS 140 cryptographic mode" on page 67
- "Trusted TCP connections" on page 68
- "Digital certificate access server (DCAS) MODIFY command for debug level" on page 69

IKE version 2 support

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

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

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

Restrictions:

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

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

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

Enabling IKE version 2 support

z/OS V1R12 Communications Server is always enabled for IKEv2 as a responder. If you want to enable the IKE daemon to initiate IPsec SAs using IKEv2 protocols, perform the task in Table 51 on page 65.

Table 51. Enabling IKE version 2 support

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

Using hash and URL encoding of certificates and certificate bundles

If you want to use hash and URL encoding of certificates and certificate bundles, perform the appropriate tasks in Table 52.

Table 52. Using hash and URL encoding of certificates and certificate bundles

Task	Reference
If you want to use hash and URL encoding of certificate bundles, create certificate bundles by defining an X.509 bundle configuration file, issuing the certbundle command, and moving the bundle file to an HTTP server.	Creating certificate bundles in *z/OS Communications Server: IP Configuration Guide*
Enable local HTTP certificate usage by the NSS server by specifying the CertificateURL parameter or the CertificateBundleURL parameter in the NSS server configuration file. When using the IBM Configuration Assistant for z/OS Communications Server, set these values from the NSS perspective in the advanced server settings for the z/OS image. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis.	• Enabling the network security services daemon to use the hash and URL certificate encoding types in *z/OS Communications Server: IP Configuration Guide* • IBM Configuration Assistant for z/OS Communications Server online helps
Enable HTTP certificate retrieval in IKED by specifying the value Allow or Tolerate on the CertificateURLLookupPreference on the KeyExchangePolicy or KeyExchangeAction statements. If you are using the IBM Configuration Assistant for z/OS Communications Server, set the default certificate URL lookup preference in the advanced stack settings of the IPSec perspective. You can modify the default mode for each connectivity rule in the advanced settings for the rule. The Configuration Assistant is available as a task in IBM z/OS Management Facility (z/OSMF) and it is also available as a standalone application that you can run on your workstation and that is supported on a best-effort basis.	• KeyExchangePolicy statement and KeyExchangeAction statement in *z/OS Communications Server: IP Configuration Reference* • IBM Configuration Assistant for z/OS Communications Server online helps

IPSec support for certificate trust chains and certificate revocation lists

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

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

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

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

Using IPSec support for certificate trust chains and certificate revocation lists

If you want to use the IPSec support for certificate trust chains and certificate revocation lists, perform the appropriate tasks in Table 53.

Table 53. IPSec support for certificate trust chains and certificate revocation lists

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

IPSec support for cryptographic currency

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

- Support for the Advanced Encryption Standard (AES) algorithm in Cipher Block Chaining (CBC) mode for IP security. In addition to the previously existing support of AES with a 128-bit key length, z/OS V1R12 Communications Server supports AES with a 256-bit key length in CBC mode. Use the longer key length for highly sensitive data.
- Support for the AES algorithm in Galois Counter Mode (GCM) and in Galois Message Authentication Code (GMAC) mode for IP security. AES in GCM mode provides both confidentiality and data origin authentication. AES-GCM is an efficient algorithm for high-speed packet networks. AES in GMAC mode provides data origin authentication but does not provide confidentiality. Use AES-GMAC when confidentiality is not needed. AES-GMAC, like AES-GCM, is also an efficient algorithm for high-speed packet networks. z/OS V1R12 Communications Server supports both 128-bit and 256-bit key lengths for these algorithms.

- Support for the use of Hashed Message Authentication Mode (HMAC) in conjunction with the SHA2-256, SHA2-384, and SHA2-512 algorithms. You can use these algorithms as the basis for data origin authentication and integrity verification. The new algorithms, HMAC-SHA2-256-128, HMAC-SHA2-384-192, and HMAC-SHA2-512-256, ensure that the data is authentic and has not been modified in transit. Versions of these algorithms that are not truncated are available as pseudorandom functions (PRFs). These algorithms are called PRF-HMAC-SHA2-256, PRF-HMAC-SHA2-384, and PRF-HMAC-SHA2-512.
- Support for an authentication algorithm, AES128-XCBC-96, that ensures the data is authentic and not modified in transit.
- Support for elliptic curve digital signature algorithm (ECDSA) authentication

Restrictions:

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

Using IPSec support for cryptographic currency

If you want to use IPSec and IKE support for cryptographic currency, perform the appropriate tasks in Table 54.

Table 54. IPSec support for cryptographic currency

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

IPSec support for FIPS 140 cryptographic mode

z/OS V1R12 Communications Server supports Federal Information Processing Standard (FIPS) 140 security requirements for cryptographic modules for IP security. This standard is useful to organizations that use cryptographic-based security systems to protect sensitive or valuable data. Protection of a cryptographic

module within a security system is necessary to maintain the confidentiality and integrity of the information that is protected by the module. FIPS 140 dictates security requirements that should be satisfied by a cryptographic module to obtain higher degrees of assurance about the integrity of the module. FIPS 140 provides four increasing, qualitative levels of security that are intended to cover a wide range of potential applications and environments. z/OS V1R12 Communications Server support is for security level 1.

Restrictions:

- Diffe-Hellman Groups 1, 2, and 5 are not supported when FIPS 140 mode is configured.
- The DES encryption algorithm and the HMAC-MD5, HMAC-MD5-96, AES128-XCBC, or AES128-XCBC-96 algorithms for authentication or pseudo-random function are not supported when FIPS 140 mode is configured.
- When FIPS 140 mode is configured, tunnels that are using the AES-GCM combined-mode encryption and authentication algorithm or tunnels that are using the AES-GMAC authentication algorithm may not be used to distribute traffic for sysplex-wide security associations (SWSA). These tunnels can be renegotiated if a DVIPA moves; however, connections to a MOVING DVIPA cannot use these tunnels. Clients connected to a MOVING DVIPA must reconnect in order to use the renegotiated tunnels.
- Certificates for RSA signature authentication that have key lengths less than 1024 bits are not supported for FIPS 140 mode.
- The use of pre-shared keys for authentication, when the keys are shorter than half the key length of the chosen authentication algorithm or pseudo-random function, are not supported for FIPS 140 mode.

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

Using the IPSec support for FIPS 140 cryptographic mode

If you want to use the IPSec support for FIPS 140 cryptographic mode, perform the appropriate tasks in Table 55.

Table 55. IPSec support for FIPS 140 cryptographic mode

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

Trusted TCP connections

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

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

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

Using trusted TCP connections

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

Table 56. Trusted TCP connections

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

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

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

Using the DCAS MODIFY command for debug level

If you want to use the DCAS MODIFY command for debug level, perform the task in Table 57.

Table 57. Digital certificate access server (DCAS) MODIFY command for debug level

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

Simplification and consumability

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

- "Enhancements to the TN3270E server"
- "IBM Health Checker for z/OS OMPROUTE checks"
- "Command to drop all connections for a server" on page 71
- "Control joining the sysplex XCF group" on page 71
- "Extension of the retry time limit for CSSMTP" on page 72

Enhancements to the TN3270E server

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

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

Using the enhancements to the TN3270E server

If you want to use the CV64 security information passed to your application, perform the task in Table 58.

Table 58. Enhancements to the TN3270E server

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

IBM Health Checker for z/OS OMPROUTE checks

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

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

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

Using the IBM Health Checker for z/OS OMPROUTE checks

If you want to use the IBM Health Checker for z/OS OMPROUTE checks, perform the task in Table 59 on page 71.

Table 59. IBM Health Checker for z/OS OMPROUTE checks

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

Command to drop all connections for a server

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

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

Using the command to drop all connections for a server

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

Table 60. Command to drop all connections for a server

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

Control joining the sysplex XCF group

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

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

Controlling joining the sysplex XCF group

If you want to control whether the TCP/IP stack joins the sysplex XCF group, perform the appropriate tasks in Table 61.

Table 61. Control joining the sysplex XCF group

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

Extension of the retry time limit for CSSMTP

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

Using the extension of the retry time limit for CSSMTP

If you want to use the longer retry time limit, perform the task in Table 62.

Table 62. Extension of the retry time limit for CSSMTP

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

SNA and Enterprise Extender

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

- "Enterprise Extender connection health verification"
- "Multipath control for Enterprise Extender" on page 73
- "Improved recovery from RTP pipe stalls" on page 73
- "Enhancements to topology database diagnostics" on page 74

Enterprise Extender connection health verification

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

Using Enterprise Extender connection health verification

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

Table 63. Enterprise Extender connection health verification

Task	Reference
Set health check verification for all EE connections by specifying the following values on the EEVERIFY start option: • ACTIVATE to verify at activation • *nnn* to verify at activation and periodically • NEVER to turn off verification	EEVERIFY start option in *z/OS Communications Server: SNA Resource Definition Reference*

Table 63. Enterprise Extender connection health verification (continued)

Task	Reference
Set health verification for a specific EE connection. • For EE connection networks, define EEVERIFY on the connection network GROUP definition statements in the EE XCA major node. • For dial-in EE connections that have their associated PUs dynamically created, define EEVERIFY on the model major node (DYNTYPE=EE) PU definition statement. • For predefined EE connections, define EEVERIFY on the PU definition statement in the switched major node.	See the following topics in *z/OS Communications Server: SNA Resource Definition Reference*: • XCA major node operand EEVERIFY • Model major node operand EEVERIFY • Switched major node operand EEVERIFY
Modify the EEVERIFY start option. Issue the MODIFY *procname*, VTAMOPTS,EEVERIFY=*value* command.	MODIFY VTAMOPTS command in *z/OS Communications Server: SNA Operation*
Display the EEVERIFY start option. Issue the DISPLAY NET,VTAMOPTS,OPTION=EEVERIFY or the DISPLAY NET,VTAMOPTS command.	DISPLAY VTAMOPTS command in *z/OS Communications Server: SNA Operation*
Display all active connections that failed EE health verification on their most recent LDLC probe. Issue the DISPLAY NET,EE,LIST=EEVERIFY command.	DISPLAY EE command in *z/OS Communications Server: SNA Operation*
Display the EE health information for the last LDLC probe that was sent to the partner. Issue the DISPLAY NET,EE,ID= command or the DISPLAY NET,EE command; specify either a host name pair or an IP address pair.	DISPLAY EE command in *z/OS Communications Server: SNA Operation*

Multipath control for Enterprise Extender

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

Controlling the multipath function for EE

To control the multipath function for EE connections, perform the appropriate tasks in Table 64.

Table 64. Multipath control for Enterprise Extender

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

Improved recovery from RTP pipe stalls

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

Enhancements to topology database diagnostics

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

Using the new topology database diagnostics

If you want to use this function, perform the appropriate tasks in Table 65.

Table 65. Enhancements to topology database diagnostics

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

System management and monitoring

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

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

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

TCP connections. The 4-tuple of a TCP connection consists of the local IP address, local port, remote IP address, and remote port for the connection.

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

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

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

- Network interface information
- Network interface and global statistics

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

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

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

GetIfStats
Provides TCP/IP network interface counters.

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

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

If you want to use this function, perform the task in Table 66.

Table 66. Enhancements to TCP/IP callable NMI (EZBNMIFR) - network interface and TCP/IP statistics

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

SMF event records for sysplex events

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

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

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

Using the SMF event records for sysplex events

If you want to use this function, perform the appropriate tasks in Table 67.

Table 67. SMF event records for sysplex events

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

Management data for CSSMTP

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

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

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

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

Using the management data for CSSMTP

If you want to use the SMF real-time data collection, perform the appropriate tasks in Table 68 on page 77.

Table 68. NMI enhancements - CSSMTP events using the NMI real-time SMF events

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

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

There are no tasks to enable application data; application data collection is always enabled. If you want to display or monitor the application data, perform the tasks in Table 69.

Table 69. CSSMTP and application data

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

Data trace records for socket data flow start and end

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

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

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

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

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

Table 70. Data trace records for socket data flow start and end

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

Enhancements to the TN3270E server - session manager sends CV64

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

Using the new session manager CV64 function

If you want to use this function, perform the appropriate tasks in Table 71.

Table 71. Enhancements to the TN3270E server - session manager sends CV64

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

Operator command to query and display OSA information

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

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

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

Using the operator command to query and display OSA information

If you want to use this function, perform the task in Table 72.

Table 72. Operator command to query and display OSA information

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

Packet trace filtering for encapsulated packets

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

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

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

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

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

Table 73. Packet trace filtering for encapsulated packets

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

Verify Netstat message catalog synchronization

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

Verifying Netstat message catalog synchronization

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

Table 74. Verify Netstat message catalog synchronization

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

Enhancements to the TCP/IP storage display

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

Using the enhancements to the TCP/IP storage display

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

Table 75. Enhancements to the TCP/IP storage display

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

Enhancements to SNMP manager API

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

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

Using the enhancements to SNMP manager API

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

Table 76. Enhancements to SNMP manager API

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

Appendix A. Related protocol specifications

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

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

For more information, contact `nic@nic.ddn.mil` or at:

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

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

See "Internet drafts" on page 97 for draft RFCs implemented in this and previous Communications Server releases.

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

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

RFC 734 *SUPDUP Protocol* M.R. Crispin

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

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

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

RFC 765 *File Transfer Protocol specification* J. Postel

RFC 768 *User Datagram Protocol* J. Postel

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

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

RFC 791 *Internet Protocol* J. Postel

RFC 792 *Internet Control Message Protocol* J. Postel

RFC 793 *Transmission Control Protocol* J. Postel

RFC 820 *Assigned numbers* J. Postel

RFC 821 *Simple Mail Transfer Protocol* J. Postel

RFC 822 *Standard for the format of ARPA Internet text messages* D. Crocker

RFC 823 *DARPA Internet gateway* R. Hinden, A. Sheltzer

RFC 826 *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware* D. Plummer

RFC 854 *Telnet Protocol Specification* J. Postel, J. Reynolds

RFC 855 *Telnet Option Specification* J. Postel, J. Reynolds

RFC 856 *Telnet Binary Transmission* J. Postel, J. Reynolds

RFC 857 *Telnet Echo Option* J. Postel, J. Reynolds

RFC 858 *Telnet Suppress Go Ahead Option* J. Postel, J. Reynolds

RFC 859 *Telnet Status Option* J. Postel, J. Reynolds

RFC 860 *Telnet Timing Mark Option* J. Postel, J. Reynolds

RFC 861 *Telnet Extended Options: List Option* J. Postel, J. Reynolds

RFC 862 *Echo Protocol* J. Postel

RFC 863 *Discard Protocol* J. Postel

RFC 864 *Character Generator Protocol* J. Postel

RFC 865 *Quote of the Day Protocol* J. Postel

RFC 868 *Time Protocol* J. Postel, K. Harrenstien

RFC 877 *Standard for the transmission of IP datagrams over public data networks* J.T. Korb

RFC 883 *Domain names: Implementation specification* P.V. Mockapetris

RFC 884 *Telnet terminal type option* M. Solomon, E. Wimmers

RFC 885 *Telnet end of record option* J. Postel

RFC 894 *Standard for the transmission of IP datagrams over Ethernet networks* C. Hornig

RFC 896 *Congestion control in IP/TCP internetworks* J. Nagle

RFC 903 *Reverse Address Resolution Protocol* R. Finlayson, T. Mann, J. Mogul, M. Theimer

RFC 904 *Exterior Gateway Protocol formal specification* D. Mills

RFC 919 *Broadcasting Internet Datagrams* J. Mogul

RFC 922 *Broadcasting Internet datagrams in the presence of subnets* J. Mogul

RFC 927 *TACACS user identification Telnet option* B.A. Anderson

RFC 933 *Output marking Telnet option* S. Silverman

RFC 946 *Telnet terminal location number option* R. Nedved

RFC 950 *Internet Standard Subnetting Procedure* J. Mogul, J. Postel

RFC 952 *DoD Internet host table specification* K. Harrenstien, M. Stahl, E. Feinler

RFC 959 *File Transfer Protocol* J. Postel, J.K. Reynolds

RFC 961 *Official ARPA-Internet protocols* J.K. Reynolds, J. Postel

RFC 974 *Mail routing and the domain system* C. Partridge

RFC 1001 *Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and methods* NetBios Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, End-to-End Services Task Force

RFC 1002 *Protocol Standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications* NetBios Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, End-to-End Services Task Force

RFC 1006 *ISO transport services on top of the TCP: Version 3* M.T. Rose, D.E. Cass

RFC 1009 *Requirements for Internet gateways* R. Braden, J. Postel

RFC 1011 *Official Internet protocols* J. Reynolds, J. Postel

RFC 1013 *X Window System Protocol, version 11: Alpha update April 1987* R. Scheifler

RFC 1014 *XDR: External Data Representation standard* Sun Microsystems

RFC 1027 *Using ARP to implement transparent subnet gateways* S. Carl-Mitchell, J. Quarterman

RFC 1032 *Domain administrators guide* M. Stahl

RFC 1033 *Domain administrators operations guide* M. Lottor

RFC 1034 *Domain names—concepts and facilities* P.V. Mockapetris

RFC 1035 *Domain names—implementation and specification* P.V. Mockapetris

RFC 1038 *Draft revised IP security option* M. St. Johns

RFC 1041 *Telnet 3270 regime option* Y. Rekhter

RFC 1042 *Standard for the transmission of IP datagrams over IEEE 802 networks* J. Postel, J. Reynolds

RFC 1043 *Telnet Data Entry Terminal option: DODIIS implementation* A. Yasuda, T. Thompson

RFC 1044 *Internet Protocol on Network System's HYPERchannel: Protocol specification* K. Hardwick, J. Lekashman

RFC 1053 *Telnet X.3 PAD option* S. Levy, T. Jacobson

RFC 1055 *Nonstandard for transmission of IP datagrams over serial lines: SLIP* J. Romkey

RFC 1057 *RPC: Remote Procedure Call Protocol Specification: Version 2* Sun Microsystems

RFC 1058 *Routing Information Protocol* C. Hedrick

RFC 1060 *Assigned numbers* J. Reynolds, J. Postel

RFC 1067 *Simple Network Management Protocol* J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin

RFC 1071 *Computing the Internet checksum* R.T. Braden, D.A. Borman, C. Partridge

RFC 1072 *TCP extensions for long-delay paths* V. Jacobson, R.T. Braden

RFC 1073 *Telnet window size option* D. Waitzman

RFC 1079 *Telnet terminal speed option* C. Hedrick

RFC 1085 *ISO presentation services on top of TCP/IP based internets* M.T. Rose

RFC 1091 *Telnet terminal-type option* J. VanBokkelen

RFC 1094 *NFS: Network File System Protocol specification* Sun Microsystems

RFC 1096 *Telnet X display location option* G. Marcy

RFC 1101 *DNS encoding of network names and other types* P. Mockapetris

RFC 1112 *Host extensions for IP multicasting* S.E. Deering

RFC 1113 *Privacy enhancement for Internet electronic mail: Part I — message encipherment and authentication procedures* J. Linn

RFC 1118 *Hitchhikers Guide to the Internet* E. Krol

RFC 1122 *Requirements for Internet Hosts—Communication Layers* R. Braden, Ed.

RFC 1123 *Requirements for Internet Hosts—Application and Support* R. Braden, Ed.

RFC 1146 *TCP alternate checksum options* J. Zweig, C. Partridge

RFC 1155 *Structure and identification of management information for TCP/IP-based internets* M. Rose, K. McCloghrie

RFC 1156 *Management Information Base for network management of TCP/IP-based internets* K. McCloghrie, M. Rose

RFC 1157 *Simple Network Management Protocol (SNMP)* J. Case, M. Fedor, M. Schoffstall, J. Davin

RFC 1158 *Management Information Base for network management of TCP/IP-based internets: MIB-II* M. Rose

RFC 1166 *Internet numbers* S. Kirkpatrick, M.K. Stahl, M. Recker

RFC 1179 *Line printer daemon protocol* L. McLaughlin

RFC 1180 *TCP/IP tutorial* T. Socolofsky, C. Kale

RFC 1183 *New DNS RR Definitions* C.F. Everhart, L.A. Mamakos, R. Ullmann, P.V. Mockapetris

RFC 1184 *Telnet Linemode Option* D. Borman

RFC 1186 *MD4 Message Digest Algorithm* R.L. Rivest

RFC 1187 *Bulk Table Retrieval with the SNMP* M. Rose, K. McCloghrie, J. Davin

RFC 1188 *Proposed Standard for the Transmission of IP Datagrams over FDDI Networks* D. Katz

RFC 1190 *Experimental Internet Stream Protocol: Version 2 (ST-II)* C. Topolcic

RFC 1191 *Path MTU discovery* J. Mogul, S. Deering

RFC 1198 *FYI on the X window system* R. Scheifler

RFC 1207 *FYI on Questions and Answers: Answers to commonly asked "experienced Internet user" questions* G. Malkin, A. Marine, J. Reynolds

RFC 1208 *Glossary of networking terms* O. Jacobsen, D. Lynch

RFC 1213 *Management Information Base for Network Management of TCP/IP-based internets: MIB-II* K. McCloghrie, M.T. Rose

RFC 1215 *Convention for defining traps for use with the SNMP* M. Rose

RFC 1227 *SNMP MUX protocol and MIB* M.T. Rose

RFC 1228 *SNMP-DPI: Simple Network Management Protocol Distributed Program Interface* G. Carpenter, B. Wijnen

RFC 1229 *Extensions to the generic-interface MIB* K. McCloghrie

RFC 1230 *IEEE 802.4 Token Bus MIB* K. McCloghrie, R. Fox

RFC 1231 *IEEE 802.5 Token Ring MIB* K. McCloghrie, R. Fox, E. Decker

RFC 1236 *IP to X.121 address mapping for DDN* L. Morales, P. Hasse

RFC 1256 *ICMP Router Discovery Messages* S. Deering, Ed.

RFC 1267 *Border Gateway Protocol 3 (BGP-3)* K. Lougheed, Y. Rekhter

RFC 1268 *Application of the Border Gateway Protocol in the Internet* Y. Rekhter, P. Gross

RFC 1269 *Definitions of Managed Objects for the Border Gateway Protocol: Version 3* S. Willis, J. Burruss

RFC 1270 *SNMP Communications Services* F. Kastenholz, ed.

RFC 1285 *FDDI Management Information Base* J. Case

RFC 1315 *Management Information Base for Frame Relay DTEs* C. Brown, F. Baker, C. Carvalho

RFC 1321 *The MD5 Message-Digest Algorithm* R. Rivest

RFC 1323 *TCP Extensions for High Performance* V. Jacobson, R. Braden, D. Borman

RFC 1325 *FYI on Questions and Answers: Answers to Commonly Asked "New Internet User" Questions* G. Malkin, A. Marine

RFC 1327 *Mapping between X.400 (1988)/ISO 10021 and RFC 822* S. Hardcastle-Kille

RFC 1340 *Assigned Numbers* J. Reynolds, J. Postel

RFC 1344 *Implications of MIME for Internet Mail Gateways* N. Bornstein

RFC 1349 *Type of Service in the Internet Protocol Suite* P. Almquist

RFC 1350 *The TFTP Protocol (Revision 2)* K.R. Sollins

RFC 1351 *SNMP Administrative Model* J. Davin, J. Galvin, K. McCloghrie

RFC 1352 *SNMP Security Protocols* J. Galvin, K. McCloghrie, J. Davin

RFC 1353 *Definitions of Managed Objects for Administration of SNMP Parties* K. McCloghrie, J. Davin, J. Galvin

RFC 1354 *IP Forwarding Table MIB* F. Baker

RFC 1356 *Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode* A. Malis, D. Robinson, R. Ullmann

RFC 1358 *Charter of the Internet Architecture Board (IAB)* L. Chapin

RFC 1363 *A Proposed Flow Specification* C. Partridge

RFC 1368 *Definition of Managed Objects for IEEE 802.3 Repeater Devices* D. McMaster, K. McCloghrie

RFC 1372 *Telnet Remote Flow Control Option* C. L. Hedrick, D. Borman

RFC 1374 *IP and ARP on HIPPI* J. Renwick, A. Nicholson

RFC 1381 *SNMP MIB Extension for X.25 LAPB* D. Throop, F. Baker

RFC 1382 *SNMP MIB Extension for the X.25 Packet Layer* D. Throop

RFC 1387 *RIP Version 2 Protocol Analysis* G. Malkin

RFC 1388 *RIP Version 2 Carrying Additional Information* G. Malkin

RFC 1389 *RIP Version 2 MIB Extensions* G. Malkin, F. Baker

RFC 1390 *Transmission of IP and ARP over FDDI Networks* D. Katz

RFC 1393 *Traceroute Using an IP Option* G. Malkin

RFC 1398 *Definitions of Managed Objects for the Ethernet-Like Interface Types* F. Kastenholz

RFC 1408 *Telnet Environment Option* D. Borman, Ed.

RFC 1413 *Identification Protocol* M. St. Johns

RFC 1416 *Telnet Authentication Option* D. Borman, ed.

RFC 1420 *SNMP over IPX* S. Bostock

RFC 1428 *Transition of Internet Mail from Just-Send-8 to 8bit-SMTP/MIME* G. Vaudreuil

RFC 1442 *Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1443 *Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1445 *Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Galvin, K. McCloghrie

RFC 1447 *Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)* K. McCloghrie, J. Galvin

RFC 1448 *Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1464 *Using the Domain Name System to Store Arbitrary String Attributes* R. Rosenbaum

RFC 1469 *IP Multicast over Token-Ring Local Area Networks* T. Pusateri

RFC 1483 *Multiprotocol Encapsulation over ATM Adaptation Layer 5* Juha Heinanen

RFC 1514 *Host Resources MIB* P. Grillo, S. Waldbusser

RFC 1516 *Definitions of Managed Objects for IEEE 802.3 Repeater Devices* D. McMaster, K. McCloghrie

RFC 1521 *MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies* N. Borenstein, N. Freed

RFC 1535 *A Security Problem and Proposed Correction With Widely Deployed DNS Software* E. Gavron

RFC 1536 *Common DNS Implementation Errors and Suggested Fixes* A. Kumar, J. Postel, C. Neuman, P. Danzig, S. Miller

RFC 1537 *Common DNS Data File Configuration Errors* P. Beertema

RFC 1540 *Internet Official Protocol Standards* J. Postel

RFC 1571 *Telnet Environment Option Interoperability Issues* D. Borman

RFC 1572 *Telnet Environment Option* S. Alexander

RFC 1573 *Evolution of the Interfaces Group of MIB-II* K. McCloghrie, F. Kastenholz

RFC 1577 *Classical IP and ARP over ATM* M. Laubach

RFC 1583 *OSPF Version 2* J. Moy

RFC 1591 *Domain Name System Structure and Delegation* J. Postel

RFC 1592 *Simple Network Management Protocol Distributed Protocol Interface Version 2.0* B. Wijnen, G. Carpenter, K. Curran, A. Sehgal, G. Waters

RFC 1594 *FYI on Questions and Answers— Answers to Commonly Asked "New Internet User" Questions* A. Marine, J. Reynolds, G. Malkin

RFC 1644 *T/TCP — TCP Extensions for Transactions Functional Specification* R. Braden

RFC 1646 *TN3270 Extensions for LUname and Printer Selection* C. Graves, T. Butts, M. Angel

RFC 1647 *TN3270 Enhancements* B. Kelly

RFC 1652 *SMTP Service Extension for 8bit-MIMEtransport* J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker

RFC 1664 *Using the Internet DNS to Distribute RFC1327 Mail Address Mapping Tables* C. Allochio, A. Bonito, B. Cole, S. Giordano, R. Hagens

RFC 1693 *An Extension to TCP: Partial Order Service* T. Connolly, P. Amer, P. Conrad

RFC 1695 *Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2* M. Ahmed, K. Tesink

RFC 1701 *Generic Routing Encapsulation (GRE)* S. Hanks, T. Li, D. Farinacci, P. Traina

RFC 1702 *Generic Routing Encapsulation over IPv4 networks* S. Hanks, T. Li, D. Farinacci, P. Traina

RFC 1706 *DNS NSAP Resource Records* B. Manning, R. Colella

RFC 1712 *DNS Encoding of Geographical Location* C. Farrell, M. Schulze, S. Pleitner D. Baldoni

RFC 1713 *Tools for DNS debugging* A. Romao

RFC 1723 *RIP Version 2—Carrying Additional Information* G. Malkin

RFC 1752 *The Recommendation for the IP Next Generation Protocol* S. Bradner, A. Mankin

RFC 1766 *Tags for the Identification of Languages* H. Alvestrand

RFC 1771 *A Border Gateway Protocol 4 (BGP-4)* Y. Rekhter, T. Li

RFC 1794 *DNS Support for Load Balancing* T. Brisco

RFC 1819 *Internet Stream Protocol Version 2 (ST2) Protocol Specification—Version ST2+* L. Delgrossi, L. Berger Eds.

RFC 1826 *IP Authentication Header* R. Atkinson

RFC 1828 *IP Authentication using Keyed MD5* P. Metzger, W. Simpson

RFC 1829 *The ESP DES-CBC Transform* P. Karn, P. Metzger, W. Simpson

RFC 1830 *SMTP Service Extensions for Transmission of Large and Binary MIME Messages* G. Vaudreuil

RFC 1831 *RPC: Remote Procedure Call Protocol Specification Version 2* R. Srinivasan

RFC 1832 *XDR: External Data Representation Standard* R. Srinivasan

RFC 1833 *Binding Protocols for ONC RPC Version 2* R. Srinivasan

RFC 1850 *OSPF Version 2 Management Information Base* F. Baker, R. Coltun

RFC 1854 *SMTP Service Extension for Command Pipelining* N. Freed

RFC 1869 *SMTP Service Extensions* J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker

RFC 1870 *SMTP Service Extension for Message Size Declaration* J. Klensin, N. Freed, K. Moore

RFC 1876 *A Means for Expressing Location Information in the Domain Name System* C. Davis, P. Vixie, T. Goodwin, I. Dickinson

RFC 1883 *Internet Protocol, Version 6 (IPv6) Specification* S. Deering, R. Hinden

RFC 1884 *IP Version 6 Addressing Architecture* R. Hinden, S. Deering, Eds.

RFC 1886 *DNS Extensions to support IP version 6* S. Thomson, C. Huitema

RFC 1888 *OSI NSAPs and IPv6* J. Bound, B. Carpenter, D. Harrington, J. Houldsworth, A. Lloyd

RFC 1891 *SMTP Service Extension for Delivery Status Notifications* K. Moore

RFC 1892 *The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages* G. Vaudreuil

RFC 1894 *An Extensible Message Format for Delivery Status Notifications*K. Moore, G. Vaudreuil

RFC 1901 *Introduction to Community-based SNMPv2* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1902 *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1903 *Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1904 *Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1905 *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1906 *Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1907 *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1908 *Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework* J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 1912 *Common DNS Operational and Configuration Errors* D. Barr

RFC 1918 *Address Allocation for Private Internets* Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear

RFC 1928 *SOCKS Protocol Version 5* M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones

RFC 1930 *Guidelines for creation, selection, and registration of an Autonomous System (AS)* J. Hawkinson, T. Bates

RFC 1939 *Post Office Protocol-Version 3* J. Myers, M. Rose

RFC 1981 *Path MTU Discovery for IP version 6* J. McCann, S. Deering, J. Mogul

RFC 1982 *Serial Number Arithmetic* R. Elz, R. Bush

RFC 1985 *SMTP Service Extension for Remote Message Queue Starting* J. De Winter

RFC 1995 *Incremental Zone Transfer in DNS* M. Ohta

RFC 1996 *A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)* P. Vixie

RFC 2010 *Operational Criteria for Root Name Servers* B. Manning, P. Vixie

RFC 2011 *SNMPv2 Management Information Base for the Internet Protocol using SMIv2* K. McCloghrie, Ed.

RFC 2012 *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2* K. McCloghrie, Ed.

RFC 2013 *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2* K. McCloghrie, Ed.

RFC 2018 *TCP Selective Acknowledgement Options* M. Mathis, J. Mahdavi, S. Floyd, A. Romanow

RFC 2026 *The Internet Standards Process — Revision 3* S. Bradner

RFC 2030 *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI* D. Mills

RFC 2033 *Local Mail Transfer Protocol* J. Myers

RFC 2034 *SMTP Service Extension for Returning Enhanced Error Codes*N. Freed

RFC 2040 *The RC5, RC5–CBC, RC-5–CBC-Pad, and RC5–CTS Algorithms*R. Baldwin, R. Rivest

RFC 2045 *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies* N. Freed, N. Borenstein

RFC 2052 *A DNS RR for specifying the location of services (DNS SRV)* A. Gulbrandsen, P. Vixie

RFC 2065 *Domain Name System Security Extensions* D. Eastlake 3rd, C. Kaufman

RFC 2066 *TELNET CHARSET Option* R. Gellens

RFC 2080 *RIPng for IPv6* G. Malkin, R. Minnear

RFC 2096 *IP Forwarding Table MIB* F. Baker

RFC 2104 *HMAC: Keyed-Hashing for Message Authentication* H. Krawczyk, M. Bellare, R. Canetti

RFC 2119 *Keywords for use in RFCs to Indicate Requirement Levels* S. Bradner

RFC 2133 *Basic Socket Interface Extensions for IPv6* R. Gilligan, S. Thomson, J. Bound, W. Stevens

RFC 2136 *Dynamic Updates in the Domain Name System (DNS UPDATE)* P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound

RFC 2137 *Secure Domain Name System Dynamic Update* D. Eastlake 3rd

RFC 2163 *Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)* C. Allocchio

RFC 2168 *Resolution of Uniform Resource Identifiers using the Domain Name System* R. Daniel, M. Mealling

RFC 2178 *OSPF Version 2* J. Moy

RFC 2181 *Clarifications to the DNS Specification* R. Elz, R. Bush

RFC 2205 *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification* R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin

RFC 2210 *The Use of RSVP with IETF Integrated Services* J. Wroclawski

RFC 2211 *Specification of the Controlled-Load Network Element Service* J. Wroclawski

RFC 2212 *Specification of Guaranteed Quality of Service* S. Shenker, C. Partridge, R. Guerin

RFC 2215 *General Characterization Parameters for Integrated Service Network Elements* S. Shenker, J. Wroclawski

RFC 2217 *Telnet Com Port Control Option* G. Clarke

RFC 2219 *Use of DNS Aliases for Network Services* M. Hamilton, R. Wright

RFC 2228 *FTP Security Extensions* M. Horowitz, S. Lunt

RFC 2230 *Key Exchange Delegation Record for the DNS* R. Atkinson

RFC 2233 *The Interfaces Group MIB using SMIv2* K. McCloghrie, F. Kastenholz

RFC 2240 *A Legal Basis for Domain Name Allocation* O. Vaughn

RFC 2246 *The TLS Protocol Version 1.0* T. Dierks, C. Allen

RFC 2251 *Lightweight Directory Access Protocol (v3)* M. Wahl, T. Howes, S. Kille

RFC 2253 *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names* M. Wahl, S. Kille, T. Howes

RFC 2254 *The String Representation of LDAP Search Filters* T. Howes

RFC 2261 *An Architecture for Describing SNMP Management Frameworks* D. Harrington, R. Presuhn, B. Wijnen

RFC 2262 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 2271 *An Architecture for Describing SNMP Management Frameworks* D. Harrington, R. Presuhn, B. Wijnen

RFC 2273 *SNMPv3 Applications* D. Levi, P. Meyer, B. Stewartz

RFC 2274 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* U. Blumenthal, B. Wijnen

RFC 2275 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* B. Wijnen, R. Presuhn, K. McCloghrie

RFC 2279 *UTF-8, a transformation format of ISO 10646* F. Yergeau

RFC 2292 *Advanced Sockets API for IPv6* W. Stevens, M. Thomas

RFC 2308 *Negative Caching of DNS Queries (DNS NCACHE)* M. Andrews

RFC 2317 *Classless IN-ADDR.ARPA delegation* H. Eidnes, G. de Groot, P. Vixie

RFC 2320 *Definitions of Managed Objects for Classical IP and ARP Over ATM Using SMIv2 (IPOA-MIB)* M. Greene, J. Luciani, K. White, T. Kuo

RFC 2328 *OSPF Version 2* J. Moy

RFC 2345 *Domain Names and Company Name Retrieval* J. Klensin, T. Wolf, G. Oglesby

RFC 2352 *A Convention for Using Legal Names as Domain Names* O. Vaughn

RFC 2355 *TN3270 Enhancements* B. Kelly

RFC 2358 *Definitions of Managed Objects for the Ethernet-like Interface Types* J. Flick, J. Johnson

RFC 2373 *IP Version 6 Addressing Architecture* R. Hinden, S. Deering

RFC 2374 *An IPv6 Aggregatable Global Unicast Address Format* R. Hinden, M. O'Dell, S. Deering

RFC 2375 *IPv6 Multicast Address Assignments* R. Hinden, S. Deering

RFC 2385 *Protection of BGP Sessions via the TCP MD5 Signature Option*A. Hefferman

RFC 2389 *Feature negotiation mechanism for the File Transfer Protocol* P. Hethmon, R. Elz

RFC 2401 *Security Architecture for Internet Protocol* S. Kent, R. Atkinson

RFC 2402 *IP Authentication Header* S. Kent, R. Atkinson

RFC 2403 *The Use of HMAC-MD5–96 within ESP and AH* C. Madson, R. Glenn

RFC 2404 *The Use of HMAC-SHA–1–96 within ESP and AH* C. Madson, R. Glenn

RFC 2405 *The ESP DES-CBC Cipher Algorithm With Explicit IV* C. Madson, N. Doraswamy

RFC 2406 *IP Encapsulating Security Payload (ESP)* S. Kent, R. Atkinson

RFC 2407 *The Internet IP Security Domain of Interpretation for ISAKMP*D. Piper

RFC 2408 *Internet Security Association and Key Management Protocol (ISAKMP)* D. Maughan, M. Schertler, M. Schneider, J. Turner

RFC 2409 *The Internet Key Exchange (IKE)* D. Harkins, D. Carrel

RFC 2410 *The NULL Encryption Algorithm and Its Use With IPsec* R. Glenn, S. Kent,

RFC 2428 *FTP Extensions for IPv6 and NATs* M. Allman, S. Ostermann, C. Metz

RFC 2445 *Internet Calendaring and Scheduling Core Object Specification (iCalendar)* F. Dawson, D. Stenerson

RFC 2459 *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* R. Housley, W. Ford, W. Polk, D. Solo

RFC 2460 *Internet Protocol, Version 6 (IPv6) Specification* S. Deering, R. Hinden

RFC 2461 *Neighbor Discovery for IP Version 6 (IPv6)* T. Narten, E. Nordmark, W. Simpson

RFC 2462 *IPv6 Stateless Address Autoconfiguration* S. Thomson, T. Narten

RFC 2463 *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification* A. Conta, S. Deering

RFC 2464 *Transmission of IPv6 Packets over Ethernet Networks* M. Crawford

RFC 2466 *Management Information Base for IP Version 6: ICMPv6 Group* D. Haskin, S. Onishi

RFC 2476 *Message Submission* R. Gellens, J. Klensin

RFC 2487 *SMTP Service Extension for Secure SMTP over TLS* P. Hoffman

RFC 2505 *Anti-Spam Recommendations for SMTP MTAs* G. Lindberg

RFC 2523 *Photuris: Extended Schemes and Attributes* P. Karn, W. Simpson

RFC 2535 *Domain Name System Security Extensions* D. Eastlake 3rd

RFC 2538 *Storing Certificates in the Domain Name System (DNS)* D. Eastlake 3rd, O. Gudmundsson

RFC 2539 *Storage of Diffie-Hellman Keys in the Domain Name System (DNS)* D. Eastlake 3rd

RFC 2540 *Detached Domain Name System (DNS) Information* D. Eastlake 3rd

RFC 2554 *SMTP Service Extension for Authentication* J. Myers

RFC 2570 *Introduction to Version 3 of the Internet-standard Network Management Framework* J. Case, R. Mundy, D. Partain, B. Stewart

RFC 2571 *An Architecture for Describing SNMP Management Frameworks* B. Wijnen, D. Harrington, R. Presuhn

RFC 2572 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 2573 *SNMP Applications* D. Levi, P. Meyer, B. Stewart

RFC 2574 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* U. Blumenthal, B. Wijnen

RFC 2575 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* B. Wijnen, R. Presuhn, K. McCloghrie

RFC 2576 *Co-Existence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* R. Frye, D. Levi, S. Routhier, B. Wijnen

RFC 2578 *Structure of Management Information Version 2 (SMIv2)* K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2579 *Textual Conventions for SMIv2* K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2580 *Conformance Statements for SMIv2* K. McCloghrie, D. Perkins, J. Schoenwaelder

RFC 2581 *TCP Congestion Control* M. Allman, V. Paxson, W. Stevens

RFC 2583 *Guidelines for Next Hop Client (NHC) Developers* R. Carlson, L. Winkler

RFC 2591 *Definitions of Managed Objects for Scheduling Management Operations* D. Levi, J. Schoenwaelder

RFC 2625 *IP and ARP over Fibre Channel* M. Rajagopal, R. Bhagwat, W. Rickard

RFC 2635 *Don't SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)* S. Hambridge, A. Lunde

RFC 2637 *Point-to-Point Tunneling Protocol* K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn

RFC 2640 *Internationalization of the File Transfer Protocol* B. Curtin

RFC 2665 *Definitions of Managed Objects for the Ethernet-like Interface Types* J. Flick, J. Johnson

RFC 2671 *Extension Mechanisms for DNS (EDNS0)* P. Vixie

RFC 2672 *Non-Terminal DNS Name Redirection* M. Crawford

RFC 2675 *IPv6 Jumbograms* D. Borman, S. Deering, R. Hinden

RFC 2710 *Multicast Listener Discovery (MLD) for IPv6* S. Deering, W. Fenner, B. Haberman

RFC 2711 *IPv6 Router Alert Option* C. Partridge, A. Jackson

RFC 2740 *OSPF for IPv6* R. Coltun, D. Ferguson, J. Moy

RFC 2753 *A Framework for Policy-based Admission Control* R. Yavatkar, D. Pendarakis, R. Guerin

RFC 2782 *A DNS RR for specifying the location of services (DNS SRV)* A. Gubrandsen, P. Vixix, L. Esibov

RFC 2821 *Simple Mail Transfer Protocol* J. Klensin, Ed.

RFC 2822 *Internet Message Format* P. Resnick, Ed.

RFC 2840 *TELNET KERMIT OPTION* J. Altman, F. da Cruz

RFC 2845 *Secret Key Transaction Authentication for DNS (TSIG)* P. Vixie, O. Gudmundsson, D. Eastlake 3rd, B. Wellington

RFC 2851 *Textual Conventions for Internet Network Addresses* M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 2852 *Deliver By SMTP Service Extension* D. Newman

RFC 2874 *DNS Extensions to Support IPv6 Address Aggregation and Renumbering* M. Crawford, C. Huitema

RFC 2915 *The Naming Authority Pointer (NAPTR) DNS Resource Record* M. Mealling, R. Daniel

RFC 2920 *SMTP Service Extension for Command Pipelining* N. Freed

RFC 2930 *Secret Key Establishment for DNS (TKEY RR)* D. Eastlake, 3rd

RFC 2941 *Telnet Authentication Option* T. Ts'o, ed., J. Altman

RFC 2942 *Telnet Authentication: Kerberos Version 5* T. Ts'o

RFC 2946 *Telnet Data Encryption Option* T. Ts'o

RFC 2952 *Telnet Encryption: DES 64 bit Cipher Feedback* T. Ts'o

RFC 2953 *Telnet Encryption: DES 64 bit Output Feedback* T. Ts'o

RFC 2992 *Analysis of an Equal-Cost Multi-Path Algorithm* C. Hopps

RFC 3019 *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol* B. Haberman, R. Worzella

RFC 3060 *Policy Core Information Model—Version 1 Specification* B. Moore, E. Ellesson, J. Strassner, A. Westerinen

RFC 3152 *Delegation of IP6.ARPA* R. Bush

RFC 3164 *The BSD Syslog Protocol* C. Lonvick

RFC 3207 *SMTP Service Extension for Secure SMTP over Transport Layer Security* P. Hoffman

RFC 3226 *DNSSEC and IPv6 A6 aware server/resolver message size requirements* O. Gudmundsson

RFC 3291 *Textual Conventions for Internet Network Addresses* M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 3363 *Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System* R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain

RFC 3376 *Internet Group Management Protocol, Version 3* B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan

RFC 3390 *Increasing TCP's Initial Window* M. Allman, S. Floyd, C. Partridge

RFC 3410 *Introduction and Applicability Statements for Internet-Standard Management Framework* J. Case, R. Mundy, D. Partain, B. Stewart

RFC 3411 *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* D. Harrington, R. Presuhn, B. Wijnen

RFC 3412 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 3413 *Simple Network Management Protocol (SNMP) Applications* D. Levi, P. Meyer, B. Stewart

RFC 3414 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* U. Blumenthal, B. Wijnen

RFC 3415 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* B. Wijnen, R. Presuhn, K. McCloghrie

RFC 3416 *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)* R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3417 *Transport Mappings for the Simple Network Management Protocol (SNMP)* R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3418 *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)* R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3419 *Textual Conventions for Transport Addresses* M. Daniele, J. Schoenwaelder

RFC 3484 *Default Address Selection for Internet Protocol version 6 (IPv6)* R. Draves

RFC 3493 *Basic Socket Interface Extensions for IPv6* R. Gilligan, S. Thomson, J. Bound, J. McCann, W. Stevens

RFC 3513 *Internet Protocol Version 6 (IPv6) Addressing Architecture* R. Hinden, S. Deering

RFC 3526 *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)* T. Kivinen, M. Kojo

RFC 3542 *Advanced Sockets Application Programming Interface (API) for IPv6* W. Richard Stevens, M. Thomas, E. Nordmark, T. Jinmei

RFC 3566 *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec* S. Frankel, H. Herbert

RFC 3569 *An Overview of Source-Specific Multicast (SSM)* S. Bhattacharyya, Ed.

RFC 3584 *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* R. Frye, D. Levi, S. Routhier, B. Wijnen

RFC 3602 *The AES-CBC Cipher Algorithm and Its Use with IPsec* S. Frankel, R. Glenn, S. Kelly

RFC 3629 *UTF-8, a transformation format of ISO 10646* R. Kermode, C. Vicisano

RFC 3658 *Delegation Signer (DS) Resource Record (RR)* O. Gudmundsson

RFC 3678 *Socket Interface Extensions for Multicast Source Filters* D. Thaler, B. Fenner, B. Quinn

RFC 3715 *IPsec-Network Address Translation (NAT) Compatibility Requirements* B. Aboba, W. Dixon

RFC 3810 *Multicast Listener Discovery Version 2 (MLDv2) for IPv6* R. Vida, Ed., L. Costa, Ed.

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

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

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

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

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

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

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

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

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

RFC 4217 *Securing FTP with TLS* P. Ford-Hutchinson

RFC 4292 *IP Forwarding Table MIB* B. Haberman

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

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

RFC 4302 *IP Authentication Header* S. Kent

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

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

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

RFC 4308 *Cryptographic Suites for IPsec* P. Hoffman

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

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

RFC 4678 *Server/Application State Protocol v1* A. Bivens

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

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

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

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

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

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

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

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

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

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

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

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

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

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 may also distribute working documents as Internet drafts. You can see Internet drafts at http://www.ietf.org/ID.html.

Several areas of IPv6 implementation include elements of the following Internet drafts and are subject to change during the RFC review process.

Draft Title and Author

draft-ietf-ipngwg-icmp-v3-07
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification A. Conta, S. Deering

Appendix B. 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, refer to 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 may view the information through the z/OS Internet Library website or the z/OS Information 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. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer 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.
1623-14 Shimotsuruma,, Yamato-Shi
Kanagawa 242-8502 Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, North Carolina 27709-2195
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or

imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

IBM is required to include the following statements in order to distribute portions of this document and the software described herein to which contributions have been made by The University of California. Portions herein © Copyright 1979, 1980, 1983, 1986, Regents of the University of California. Reproduced by permission. Portions herein were developed at the Electrical Engineering and Computer Sciences Department at the Berkeley campus of the University of California under the auspices of the Regents of the University of California.

Portions of this publication relating to RPC are Copyright © Sun Microsystems, Inc., 1988, 1989.

Some portions of this publication relating to X Window System** are Copyright © 1987, 1988 by Digital Equipment Corporation, Maynard, Massachusetts, and the Massachusetts Institute Of Technology, Cambridge, Massachusetts. All Rights Reserved.

Some portions of this publication relating to X Window System are Copyright © 1986, 1987, 1988 by Hewlett-Packard Corporation.

Permission to use, copy, modify, and distribute the M.I.T., Digital Equipment Corporation, and Hewlett-Packard Corporation portions of this software and its documentation for any purpose without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T., Digital, and Hewlett-Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T., Digital, and Hewlett-Packard make no representation about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright © 1983, 1995-1997 Eric P. Allman

Copyright © 1988, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

```
This product includes software developed by the University of
California, Berkeley and its contributors.
```

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software program contains code, and/or derivatives or modifications of code originating from the software program "Popper." Popper is Copyright ©1989-1991 The Regents of the University of California, All Rights Reserved. Popper was created by Austin Shelton, Information Systems and Technology, University of California, Berkeley.

Permission from the Regents of the University of California to use, copy, modify, and distribute the "Popper" software contained herein for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies. HOWEVER, ADDITIONAL PERMISSIONS MAY BE NECESSARY FROM OTHER PERSONS OR ENTITIES, TO USE DERIVATIVES OR MODIFICATIONS OF POPPER.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THE POPPER SOFTWARE, OR ITS DERIVATIVES OR MODIFICATIONS, AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE POPPER SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

Copyright © 1983 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to

endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   ```
   This product includes software developed by the University of
   California, Berkeley and its contributors.
   ```

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original M.I.T. software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

This product includes cryptographic software written by Eric Young.

Copyright © 1999, 2000 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 2004 IBM Corporation and its licensors, including Sendmail, Inc., and the Regents of the University of California. All rights reserved.

Copyright © 1999,2000,2001 Compaq Computer Corporation

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

You can obtain softcopy from the z/OS Collection (SK3T-4269), which contains BookManager and PDF formats.

Policy for unsupported hardware

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

Trademarks

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

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

PostScript is a registered trademark 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. In addition, Info APARs for z/OS documents are in *z/OS and z/OS.e DOC APAR and PTF ++HOLD Documentation*, which can be found at http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/ BOOKS/ZIDOCMST/CCONTENTS.

z/OS Communications Server information

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

Planning

Title	Number	Description
z/OS Communications Server: New Function Summary	GC31-8771	This document is intended to help you plan for new IP for SNA function, whether you are migrating from a previous version or installing z/OS for the first time. It summarizes what is new in the release and identifies the suggested and required modifications needed to use the enhanced functions.
z/OS Communications Server: IPv6 Network and Application Design Guide	SC31-8885	This document is a high-level introduction to IPv6. It describes concepts of z/OS Communications Server's support of IPv6, coexistence with IPv4, and migration issues.

Resource definition, configuration, and tuning

Title	Number	Description
z/OS Communications Server: IP Configuration Guide	SC31-8775	This document describes the major concepts involved in understanding and configuring an IP network. Familiarity with the z/OS operating system, IP protocols, z/OS UNIX System Services, and IBM Time Sharing Option (TSO) is recommended. Use this document in conjunction with the *z/OS Communications Server: IP Configuration Reference*.

Title	Number	Description
z/OS Communications Server: IP Configuration Reference	SC31-8776	This document presents information for people who want to administer and maintain IP. Use this document in conjunction with the *z/OS Communications Server: IP Configuration Guide*. The information in this document includes: • TCP/IP configuration data sets • Configuration statements • Translation tables • Protocol number and port assignments
z/OS Communications Server: SNA Network Implementation Guide	SC31-8777	This document presents the major concepts involved in implementing an SNA network. Use this document in conjunction with the *z/OS Communications Server: SNA Resource Definition Reference*.
z/OS Communications Server: SNA Resource Definition Reference	SC31-8778	This document describes each SNA definition statement, start option, and macroinstruction for user tables. It also describes NCP definition statements that affect SNA. Use this document in conjunction with the *z/OS Communications Server: SNA Network Implementation Guide*.
z/OS Communications Server: SNA Resource Definition Samples	SC31-8836	This document contains sample definitions to help you implement SNA functions in your networks, and includes sample major node definitions.
z/OS Communications Server: IP Network Print Facility	SC31-8833	This document is for system programmers and network administrators who need to prepare their network to route SNA, JES2, or JES3 printer output to remote printers using TCP/IP Services.

Operation

Title	Number	Description
z/OS Communications Server: IP User's Guide and Commands	SC31-8780	This document describes how to use TCP/IP applications. It contains requests that allow a user to log on to a remote host using Telnet, transfer data sets using FTP, send and receive electronic mail, print on remote printers, and authenticate network users.
z/OS Communications Server: IP System Administrator's Commands	SC31-8781	This document describes the functions and commands helpful in configuring or monitoring your system. It contains system administrator's commands, such as TSO NETSTAT, PING, TRACERTE and their UNIX counterparts. It also includes TSO and MVS commands commonly used during the IP configuration process.
z/OS Communications Server: SNA Operation	SC31-8779	This document serves as a reference for programmers and operators requiring detailed information about specific operator commands.
z/OS Communications Server: Quick Reference	SX75-0124	This document contains essential information about SNA and IP commands.

Customization

Title	Number	Description
z/OS Communications Server: SNA Customization	SC31-6854	This document enables you to customize SNA, and includes the following: • Communication network management (CNM) routing table • Logon-interpret routine requirements • Logon manager installation-wide exit routine for the CLU search exit • TSO/SNA installation-wide exit routines • SNA installation-wide exit routines

Writing application programs

Title	Number	Description
z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference	SC31-8788	This document describes the syntax and semantics of program source code necessary to write your own application programming interface (API) into TCP/IP. You can use this interface as the communication base for writing your own client or server application. You can also use this document to adapt your existing applications to communicate with each other using sockets over TCP/IP.
z/OS Communications Server: IP CICS Sockets Guide	SC31-8807	This document is for programmers who want to set up, write application programs for, and diagnose problems with the socket interface for CICS using z/OS TCP/IP.
z/OS Communications Server: IP IMS Sockets Guide	SC31-8830	This document is for programmers who want application programs that use the IMS TCP/IP application development services provided by the TCP/IP Services of IBM.
z/OS Communications Server: IP Programmer's Guide and Reference	SC31-8787	This document describes the syntax and semantics of a set of high-level application functions that you can use to program your own applications in a TCP/IP environment. These functions provide support for application facilities, such as user authentication, distributed databases, distributed processing, network management, and device sharing. Familiarity with the z/OS operating system, TCP/IP protocols, and IBM Time Sharing Option (TSO) is recommended.
z/OS Communications Server: SNA Programming	SC31-8829	This document describes how to use SNA macroinstructions to send data to and receive data from (1) a terminal in either the same or a different domain, or (2) another application program in either the same or a different domain.
z/OS Communications Server: SNA Programmer's LU 6.2 Guide	SC31-8811	This document describes how to use the SNA LU 6.2 application programming interface for host application programs. This document applies to programs that use only LU 6.2 sessions or that use LU 6.2 sessions along with other session types. (Only LU 6.2 sessions are covered in this document.)
z/OS Communications Server: SNA Programmer's LU 6.2 Reference	SC31-8810	This document provides reference material for the SNA LU 6.2 programming interface for host application programs.
z/OS Communications Server: CSM Guide	SC31-8808	This document describes how applications use the communications storage manager.

Title	Number	Description
z/OS Communications Server: CMIP Services and Topology Agent Guide	SC31-8828	This document describes the Common Management Information Protocol (CMIP) programming interface for application programmers to use in coding CMIP application programs. The document provides guide and reference information about CMIP services and the SNA topology agent.

Diagnosis

Title	Number	Description
z/OS Communications Server: IP Diagnosis Guide	GC31-8782	This document explains how to diagnose TCP/IP problems and how to determine whether a specific problem is in the TCP/IP product code. It explains how to gather information for and describe problems to the IBM Software Support Center.
z/OS Communications Server: ACF/TAP Trace Analysis Handbook	GC23-8588-00	This document explains how to gather the trace data that is collected and stored in the host processor. It also explains how to use the Advanced Communications Function/Trace Analysis Program (ACF/TAP) service aid to produce reports for analyzing the trace data information.
z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures and *z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT*	GC31-6850 GC31-6851	These documents help you identify an SNA problem, classify it, and collect information about it before you call the IBM Support Center. The information collected includes traces, dumps, and other problem documentation.
z/OS Communications Server: SNA Data Areas Volume 1 and *z/OS Communications Server: SNA Data Areas Volume 2*	GC31-6852 GC31-6853	These documents describe SNA data areas and can be used to read an SNA dump. They are intended for IBM programming service representatives and customer personnel who are diagnosing problems with SNA.

Messages and codes

Title	Number	Description
z/OS Communications Server: SNA Messages	SC31-8790	This document describes the ELM, IKT, IST, IUT, IVT, and USS messages. Other information in this document includes: • Command and RU types in SNA messages • Node and ID types in SNA messages • Supplemental message-related information
z/OS Communications Server: IP Messages Volume 1 (EZA)	SC31-8783	This volume contains TCP/IP messages beginning with EZA.
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	SC31-8784	This volume contains TCP/IP messages beginning with EZB or EZD.
z/OS Communications Server: IP Messages Volume 3 (EZY)	SC31-8785	This volume contains TCP/IP messages beginning with EZY.
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	SC31-8786	This volume contains TCP/IP messages beginning with EZZ and SNM.
z/OS Communications Server: IP and SNA Codes	SC31-8791	This document describes codes and other information that appear in z/OS Communications Server messages.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Communicating your comments to IBM

If you especially like or dislike anything about this document, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this document. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

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

Please send your comments to us in either of the following ways:

- If you prefer to send comments by FAX, use this number: 1+919-254-1258
- If you prefer to send comments electronically, use this address:
  - comsvrcf@us.ibm.com
- If you prefer to send comments by post, use this address:

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

Make sure to include the following in your note:

- Title and publication number of this document
- Page number or topic to which your comment applies.

Program Number: 5694–A01

Printed in USA

GC31-8771-07