z/OS Communications Server

New Function Summary

Version 1 Release 6

GC31-8771-00

z/OS Communications Server

New Function Summary

Version 1 Release 6

GC31-8771-00

Note:
Before using this information and the product it supports, be sure to read the general information under "Notices" on page 269.

First Edition (September 2004)

This edition applies to Version 1 Release 6 of z/OS (5694-A01) and Version 1 Release 6 of z/OS.e (5655-G52) 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+919-254-4028

Internet e-mail:

- comsvrcf@us.ibm.com

World Wide Web:
http://www.ibm.com/servers/eserver/zseries/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 6 Communications Server (z/OS Communications Server), including the exploitation considerations of the following earlier releases:

- z/OS V1R5 Communications Server
- z/OS V1R4 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 supports z/OS.e.

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 the following sections:

- Chapter 1, “Planning to use new functions,” on page 3 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.
- Part 2, “IP functions,” on page 23 includes the following chapters:
  - Chapter 2, “Roadmap to IP functions,” on page 25 provides a roadmap of the IP functional enhancements introduced in z/OS V1R6 Communications

Server, z/OS V1R5 Communications Server and z/OS V1R4 Communications Server. Each entry indicates whether enabling or actions are required, and page references.
  - Chapter 3, "V1R6 IP new function summary," on page 29 summarizes the IP functions and migration considerations of z/OS V1R6 Communications Server.
  - Chapter 4, "V1R5 IP new function summary," on page 63 summarizes the IP functions and migration considerations of z/OS V1R5 Communications Server.
  - Chapter 5, "V1R4 IP new function summary," on page 133 summarizes the IP functions and migration considerations of z/OS V1R4 Communications Server.
- Part 3, "SNA functions," on page 175 includes the following chapters:
  - Chapter 6, "Roadmap to SNA functions," on page 177 provides a roadmap of the SNA functional enhancements introduced in z/OS V1R6 Communications Server, z/OS V1R5 Communications Server and z/OS V1R4 Communications Server. Each entry indicates whether enabling or actions are required, and page references.
  - Chapter 7, "V1R6 SNA new function summary," on page 179 summarizes the SNA functions and migration considerations of z/OS V1R6 Communications Server.
  - Chapter 8, "V1R5 SNA new function summary," on page 203 summarizes the SNA functions and migration considerations of z/OS V1R5 Communications Server.
  - Chapter 9, "V1R4 SNA new function summary," on page 231 summarizes the SNA functions and migration considerations of z/OS V1R4 Communications Server.
- Part 4 includes the following appendixes:
  - Appendix A, "Related protocol specifications (RFCs)," on page 251 lists the related protocol specifications for TCP/IP.
  - Appendix B, "Architectural specifications," on page 261 lists documents that provide architectural specifications for the SNA Protocol.
  - Appendix C, "Information APARs," on page 263 lists information APARs for IP and SNA documents.
  - Appendix D, "Accessibility," on page 267 describes accessibility features to help users with physical disabilities.
- "Bibliography" on page 279 contains descriptions of the documents in the z/OS Communications Server library.
- "Notices" on page 269 contains notices and trademarks used in this document.

How to use this document

Use this document as an introduction to every function and enhancement of the past three releases of z/OS Communications Server.

The roadmap chapters show you a list of the functions of the past three releases. Use the roadmaps to see a release at a glance and to determine which functions have tasks that are necessary to exploit the functions.

Use the function summary chapters to learn about the following 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

Use the appendixes to learn about additional topics that might interest you.

Determining if a publication is current

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

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

How to contact IBM service

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

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

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

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

If you would like to provide feedback on this publication, see "Communicating Your Comments to IBM" on page 293.

Conventions and terminology used in this document

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

Clarification of notes

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

Note Supplemental detail

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

Guideline
Customary way to perform a procedure; stronger request than recommendation

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 "z/OS Communications Server information" on page 279, 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.

Related information

This section contains subsections on:

Softcopy information

Softcopy publications are available in the following collections:

Titles	Order Number	Description
z/OS V1R6 Collection	SK3T-4269	This is the CD collection shipped with the z/OS product. It includes the libraries for z/OS V1R6, in both BookManager and PDF formats.

Titles	Order Number	Description
z/OS Software Products Collection	SK3T-4270	This CD includes, in both BookManager and PDF formats, the libraries of z/OS software products that run on z/OS but are not elements and features, as well as the *Getting Started with Parallel Sysplex®* bookshelf.
z/OS V1R6 and Software Products DVD Collection	SK3T-4271	This collection includes the libraries of z/OS (the element and feature libraries) and the libraries for z/OS software products in both BookManager and PDF format. This collection combines SK3T-4269 and SK3T-4270.
z/OS Licensed Product Library	SK3T-4307	This CD includes the licensed documents in both BookManager and PDF format.
System Center Publication IBM S/390® Redbooks™ Collection	SK2T-2177	This collection contains over 300 ITSO redbooks that apply to the S/390 platform and to host networking arranged into subject bookshelves.

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 may be helpful to readers.

Title	Number
z/OS Integrated Security Services Firewall Technologies	SC24-5922
S/390: OSA-Express Customer's Guide and Reference	SA22-7403
z/OS JES2 Initialization and Tuning Guide	SA22-7532
z/OS MVS Diagnosis: Procedures	GA22-7587
z/OS MVS Diagnosis: Reference	GA22-7588
z/OS MVS Diagnosis: Tools and Service Aids	GA22-7589
z/OS Integrated Security Services LDAP Client Programming	SC24-5924
z/OS Integrated Security Services LDAP Server Administration and Use	SC24-5923
Understanding LDAP	SG24-4986
z/OS UNIX System Services Programming: Assembler Callable Services Reference	SA22-7803
z/OS UNIX System Services Command Reference	SA22-7802
z/OS UNIX System Services User's Guide	SA22-7801
z/OS UNIX System Services Planning	GA22-7800
z/OS MVS Using the Subsystem Interface	SA22-7642
z/OS C/C++ Run-Time Library Reference	SA22-7821
z/OS Program Directory	GI10-0670
DNS and BIND, Fourth Edition, O'Reilly and Associates, 2001	ISBN 0-596-00158-4
Routing in the Internet , Christian Huitema (Prentice Hall PTR, 1995)	ISBN 0-13-132192-7
sendmail, Bryan Costales and Eric Allman, O'Reilly and Associates, 2002	ISBN 1-56592-839-3

Title	Number
TCP/IP Tutorial and Technical Overview	GG24-3376
TCP/IP Illustrated, Volume I: The Protocols, W. Richard Stevens, Addison-Wesley Publishing, 1994	ISBN 0-201-63346-9
TCP/IP Illustrated, Volume II: The Implementation, Gary R. Wright and W. Richard Stevens, Addison-Wesley Publishing, 1995	ISBN 0-201-63354-X
TCP/IP Illustrated, Volume III, W. Richard Stevens, Addison-Wesley Publishing, 1995	ISBN 0-201-63495-3
z/OS Crytographic Service System Secure Sockets Layer Programming	SC24-5901
SNA Formats	GA27-3136

Redbooks

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

Title	Number
TCP/IP Tutorial and Technical Overview	GG24–3376
SNA and TCP/IP Integration	SG24–5291
IBM Communications Server for OS/390® V2R10 TCP/IP Implementation Guide: Volume 1: Configuration and Routing	SG24–5227
IBM Communications Server for OS/390 V2R10 TCP/IP Implementation Guide: Volume 2: UNIX Applications	SG24–5228
IBM Communications Server for OS/390 V2R7 TCP/IP Implementation Guide: Volume 3: MVS Applications	SG24–5229
Secureway Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements	SG24–5631
TCP/IP in a Sysplex	SG24–5235
Managing OS/390 TCP/IP with SNMP	SG24–5866
Security in OS/390–based TCP/IP Networks	SG24–5383
IP Network Design Guide	SG24–2580
Migrating Subarea Networks to an IP Infrastructure	SG24–5957
IBM Communication Controller Migration Guide	SG24–6298

Where to find related information on the Internet

z/OS

– http://www.ibm.com/servers/eserver/zseries/zos/

z/OS Internet Library

– http://www.ibm.com/servers/eserver/zseries/zos/bkserv/

IBM Communications Server product

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

IBM Communications Server product support

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

IBM Systems Center publications

– http://www.redbooks.ibm.com/

IBM Systems Center flashes

– http://www-1.ibm.com/support/techdocs/atsmastr.nsf

RFCs

– http://www.ietf.org/rfc.html

Internet drafts

– http://www.ietf.org/ID.html

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

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

USENET news groups:
comp.protocols.dns.bind

For BIND mailing lists, see:

- http://www.isc.org/ml-archives/
  - BIND Users
    - Subscribe by sending mail to bind-users-request@isc.org.
    - Submit questions or answers to this forum by sending mail to bind-users@isc.org.
  - BIND 9 Users (Note: This list may not be maintained indefinitely.)
    - Subscribe by sending mail to bind9-users-request@isc.org.
    - Submit questions or answers to this forum by sending mail to bind9-users@isc.org.

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

Accessing z/OS licensed documents on the Internet

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

http://www.ibm.com/servers/resourcelink

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

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

http://www.ibm.com/servers/resourcelink

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

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

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

Printed licensed documents are not available from IBM.

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

Using LookAt to look up message explanations

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

You can use LookAt from the following locations to find IBM message explanations for z/OS elements and features, z/VM®, and VSE:

- The Internet. You can access IBM message explanations directly from the LookAt Web site at http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/.
- Your z/OS TSO/E host system. You can install code on your z/OS or z/OS.e® systems to access IBM message explanations, using LookAt from a TSO/E command line (for example, TSO/E prompt, ISPF, or z/OS UNIX System Services running OMVS).
- Your Microsoft® Windows® workstation. You can install code to access IBM message explanations on the *z/OS Collection* (SK3T-4269), using LookAt from a Microsoft Windows DOS command line.
- Your wireless handheld device. You can use the LookAt Mobile Edition with a handheld device that has wireless access and an Internet browser (for example, Internet Explorer for Pocket PCs, Blazer, or Eudora for Palm OS, or Opera for Linux handheld devices). Link to the LookAt Mobile Edition from the LookAt Web site.

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from a disk on your *z/OS Collection* (SK3T-4269), or from the LookAt Web site (click **Download**, and select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.

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:

- Go to the z/OS contact page at:

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

  There you will find the feedback page where you can enter and submit your comments.
- Send your comments by e-mail to comsvrcf@us.ibm.com. Be sure to include the name of the document, the part number of the document, the version of z/OS Communications Server, and, if applicable, the specific location of the text you are commenting on (for example, a section number, a page number or a table number).

Summary of changes

Summary of changes
for GC31-8771-00
z/OS Version 1 Release 6

This document contains information previously presented in:

- *z/OS V1R5 Communications Server: IP Migration and Exploitation*, GC31-8773-03
- *z/OS V1R5 Communications Server: SNA Migration and Exploitation*, GC31-8774-03

Those documents do not exist for z/OS Version 1 Release 6. This document replaces them for the following reasons:

- Migration, interface changes, and high level functional descriptions are presented in z/OS system books:
  - *z/OS Migration*, GA22-7499-05
  - *z/OS Summary of Message and Interface Changes*, SA22-7505-06
  - *z/OS Introduction and Release Guide*, GA22-7502-07
- It is not necessary to duplicate information in Communications Server documents. At the same time, Communications Server is dedicated to providing detailed information that describes how to use our functions. This document combines the two components of Communications Server, IP and SNA, and presents exploitation information for the current and past two releases.

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.

Retained information

The following information was retained from *IP Migration and Exploitation*, GC31-8773-03:

- The TCP/IP packaging process section
- The encryption features section
- The planning checklist
- The roadmap table that lists the functional enhancements for each release
- The IP release summary sections for z/OS V1R4 Communications Server and z/OS V1R5 Communications Server

  Note: The FTP, Telnet, SNMP, and DNS sections are merged with the general release functional descriptions. They are no longer in separate, application-specific chapters.

The following information was retained from *SNA Migration and Exploitation*, GC31-8774-03:

- The defining data sets section
- The SNA release summary sections for z/OS V1R4 Communications Server and z/OS V1R5 Communications Server, with the exception of the "New and changed interfaces that enable use of this function" sections. The interface information is presented in *z/OS Summary of Message and Interface Changes* and is not duplicated in this new document.

New information

- Chapter 3, "V1R6 IP new function summary," on page 29 includes descriptions and exploitation procedures for the new IP functions and enhancements introduced in this release.
- Chapter 7, "V1R6 SNA new function summary," on page 179 includes descriptions and exploitation procedures for the new SNA functions and enhancements introduced in this release.
- Select examples and tasks are enabled for z/OS library center advanced searches.

Moved information

- The following information was moved from *IP Migration and Exploitation*, GC31-8773-03 to *z/OS Communications Server: IP Configuration Guide*:
  - Product overview information.
  - The migrating from Community-Based Security to SNMPv3 appendix. It was moved to the following Web site: Migrating z/OS SNMP to SNMPv3.
- The following information was moved from *SNA Migration and Exploitation*, GC31-8774-03:
  - Selected post-installation consideration sections:
    - Defining z/OS V1R5 Communications Server to z/OS
    - Using automatic restart manager
    - Starting z/OS Communications Server

    They were moved to *z/OS Communications Server: SNA Network Implementation Guide*.
  - The section on installing dump analysis and VIT analysis tools. It was moved to *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*.
  - The storage estimate worksheets. They were moved to *z/OS Communications Server: SNA Network Implementation Guide*.

Deleted information

- The upgrading chapters of *SNA Migration and Exploitation*, GC31-8774-03 are not included in this document because that information now exists in z/OS system level documents. Specifically, the information that described how to maintain the behavior of the SNA functions of previous releases is in *z/OS Migration*. The upgrading user interfaces information is in *z/OS Summary of Message and Interface Changes*.
- You can still access the deleted information by referring to the V1R5 documentation for *IP Migration and Exploitation*, GC31-8773-03 and *SNA Migration and Exploitation*, GC31-8774-03 at the following Web site: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/.

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

Part 1. Planning

Chapter 1. Planning to use new functions

This chapter includes the following sections to 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. For more information on z/OS Communications Server IP protocols, refer to *z/OS Communications Server: IP Configuration Guide*.

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. For more information on z/OS Communications Server SNA protocols, refer to *z/OS Communications Server: SNA Network Implementation Guide*.

For the purposes of this library, zSeries® is defined to mean the hardware that is known as the IBM S/390 Parallel Enterprise Server™ Generation 5 (G5) and Generation 6 (G6), the IBM S/390 Multiprise® 3000 Enterprise Server, as well as the IBM @server zSeries 800 (z800), 900 (z900), and 990 (z990).

The z800, z900 and z990 servers are also known as z/Architecture™ servers. z/OS V1R6 is an architectural level-set; it will only run in z/Architecture mode on z/Architecture servers. G5, G6 and Multiprise 3000 servers are not supported for z/OS V1R6.

How to determine which documents to use as you migrate

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

Table 1. Table comparing documents used in migration

z/OS and z/OS.e 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 or individual elements and features of z/OS.**
z/OS Communications Server: New Function Summary	This document includes function summary chapters 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, refer to the *z/OS Information Roadmap*.

IP encryption features

Encryption features are available for IP at no additional cost, but must be ordered separately from the z/OS base. Level 3 is the only level available for ordering with z/OS V1R6 Communications Server.

The encryption features include the following capabilities:

Level 1
This level of encryption is included in the base of z/OS V1R6 Communications Server.

Level 2
This level of encryption is included in the base of z/OS V1R6 Communications Server and offers IP Security (IPSec) DES/CDMF and SNMPv3 56 bit DES.

Level 3

This level of encryption is shipped, if ordered, as FMID JIP615K and offers IPSec Triple DES.

Planning checklist

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

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

__ 2. Understand that z/OS V1R6 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 "How to determine which documents to use as you migrate" on page 3.

For information about installation, see the following 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, refer to the *z/OS Program Directory* and the appropriate INFO APAR on RETAIN® (see Appendix C, "Information APARs," on page 263 for the APAR numbers). You can also refer to the storage estimate worksheets in *z/OS Communications Server: SNA Network Implementation Guide*.

__ 3. Develop your education plan:
- Evaluate the z/OS V1R6 Communications Server features and enhancements by reading the new function chapters in this document. Plan which new functions will be incorporated into your system.
- Order the appropriate publications.

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

__ 5. Read the hints, tips, and so on found at www-4.ibm.com /software/network/commserver/support.

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

__ 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, refer to *z/OS and z/OS.e Planning for Installation*.

__ 9. Complete post-installation activities:
- Use the *z/OS Communications Server: IP Configuration Guide* to customize your TCP/IP system.
- Use the *z/OS Communications Server: SNA Customization*, *z/OS Communications Server: SNA Network Implementation Guide*, and *z/OS Communications Server: SNA Resource Definition Reference* to customize your SNA system.
- 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 V1R6 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 "HFS files" on page 8.

MVS data sets

Table 2 lists the distribution library data sets required by z/OS V1R6 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 includes
AEZAMODS	Distribution library for base link-edit modules
AEZARNT1	Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS
AEZARNT4	Reentrant object modules for RPC
AEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)
AEZASMP1	Sample source programs, catalog procedures, CLIST, and installation jobs
AEZAXLTD	Translated default tables
AEZAXLTK	Translated Kanji, Hangeul, and Traditional Chinese DBCS tables and codefiles
AEZAXLT1	Translation table SBCS source and DBCS source for Hangeul and Traditional Chinese
AEZAXLT2	TELNET client translation tables

Table 2. Distribution library data sets (continued)

Data set	Description
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 V1R6 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
SEZADEFS	Used for Sidedecks
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
SEZAINST	Installation samples and related members
SEZALIBN	NCS library system library
SEZALOAD	Executable load modules for concatenation to LINKLIB
SEZALNK2	LB@ADMIN for the NCS administrator
SEZALPA	Executable load modules for concatenation to LPALIB
SEZAMENU	Messages for the Network Print Facility and IPCS
SEZANCLS	SNMP CLISTs
SEZANMAC	C headers and assembler macros for z/OS UNIX and TCP/IP Services APIs
SEZANPNL	SNMP panels
SEZAOLDX	X Window System library (X10 compatibility routines)
SEZAPENU	ISPF panels for the Network Print Facility and IPCS
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

Table 3. Target library data sets (continued)

Data set	Description
SEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)
SEZAROE2	Reentrant object module for SEZAXAWL (OS/390 UNIX support)
SEZAROE3	Reentrant object module for SEZAXMLB (OS/390 UNIX support)
SEZARPCL	Remote procedure call library
SEZATCP	Executable load modules for STEPLIB or LINKLIB concatenation
SEZATCPX	Source for the country SBCS translation tables
SEZATELX	Source for the TELNET country translation tables
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	OSF/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 V1R6 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.SBLSCLI0	Contains CLISTs and REXX execs
SYS1.SBLSMSGS	Contains messages
SYS1.SBLSPNL0	Dialog panels for the interactive problem control system (IPCS) dialog programs
SYS1.SBLSTBL0	Contains tables, keys, and commands
SYS1.SCIMXML / SYS1.ACIMPLUG	Managed System Infrastructure Product Definition XML

HFS files

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

Defining SNA data sets

This section describes z/OS data sets that you need to define or modify for z/OS V1R6 Communications Server. Table 5 shows the z/OS data sets that contain information for z/OS V1R6 Communications Server, and Table 6 on page 11 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. For more information, refer to *z/OS Communications Server: IP Configuration Guide*.

The following sections 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.
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 and APPC Application Suite application program interface headers	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.

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

Name of data set	Contents	Comments
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.SAPPDAT2	APPC Application Suite messages	Required for APPC Application Suite.
SYS1.SAPPDAT4	APPC Application Suite ANAME database skeleton	Required for APPC Application Suite.
SYS1.SAPPMOD1	APPC Application Suite load modules	Required for APPC Application Suite.
SYS1.AAPPMOD2	APPC Application Suite API load modules	Required for APPC Application Suite.
SYS1.SAPPSAMP	APPC Application Suite installation and execution samples	Required for APPC Application Suite.
SYS1.SBLSCLI0	Command lists and REXX execs	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. Seez/*OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures* for more information.
SYS1.SBLSMSG0	Compiled messages	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	Compiled panels	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	Compiled tables, keylists, and commands	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 13 for a description.
SYS1.SISTCLIB	z/OS Communications Server load modules to be loaded into common service area and extended common service area (CSA/ECSA) storage	Required.
SYS1.SISTCMIP	Directory definition file. The member name of the directory definition file is ACYDDF.	Required for CMIP services. See "SYS1.SISTCMIP" on page 13 for a description.
SYS1.SISTDAT1	Online tools	Optional. Use this library only if you intend to use the online information tools shipped with z/OS Communications Server.

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

Name of data set	Contents	Comments
SYS1.SISTDAT2	Message skeleton file for translation	Required. Refer to *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, refer to 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.
SYS1.SSPLIB	NCP loader utility program	Required; added when NCP is installed. Refer to "SYS1.SSPLIB" on page 21 for information on SYS1.SSPLIB requirements.
	NCP dump utility program	Required; added when NCP is installed. Refer to "SYS1.SSPLIB" on page 21 for information on SYS1.SSPLIB requirements.
	NCP dump bootstrap program	Required; added when NCP is installed. Refer to "SYS1.SSPLIB" on page 21 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. Created during system generation. Must be listed in an IEAAPFxx parmlib member.

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

Name of data set	Contents	Comments
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 V1R6 Communications Server

This section describes data sets that contain information for z/OS V1R6 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 the following:

1. Allocate the SYS1.SISTCLIB data set using a utility program, and catalog the data set before SMP/E installation. Refer to 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 and BLKSIZE for this file are both 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 the following 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 and BLKSIZE for this file are both 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 the following 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 the following:

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. For more information about start options, refer to *z/OS Communications Server: SNA Network Implementation Guide*.
2. Specify the DD name for SYS1.VTAMLST as VTAMLST. You should specify the following 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, refer to *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. Two sets of IBM-supplied CoS definitions are available:

- COSAPPN

  The definitions in COSAPPN are made up of 8-row LINEROW entries for all Classes of Service and are appropriate for most sessions.
- ISTACST2

  The definitions in ISTACST2 are made up of 8-row LINEROW entries for all Classes of Service except #BATCH, #BATCHSC, #INTER, and #INTERSC (which are made up of 12-row entries) and 8-row NODEROW entries for all Classes of Service. Twelve-row LINEROW entries better enable z/OS Communications Server to select an optimal route for a session. This is most useful for multiple types of connections with different TG characteristics. For example, this is useful when channel-to-channel, token ring network, FDDI LAN, or ATM are used in the network.

Either COSAPPN or ISTACST2 is required if z/OS Communications Server is configured as an APPN node. To use COSAPPN or ISTACST2, 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 both sets of definitions into SYS1.VTAMLST, but you can have only one set active at any time.

COSAPPN is automatically activated when z/OS Communications Server is initialized. If you choose to use ISTACST2, you must use the **VARY ACT** command to activate it, or place the ISTACST2 member in the configuration list to automatically activate it at z/OS Communications Server initialization. You can rename the IBM-supplied sets of definitions so that ISTACST2 is named COSAPPN and COSAPPN is either not used or is renamed to something else. This enables the set of definitions with 12-row LINEROW entries to be automatically activated at initialization.

Very Important: With 12-row LINEROW entries, you should have a set of definitions with 12-row LINEROW entries activated on each network node in the network for optimal routing in networks that include ATM native connections.

Not all HPR APPN products support CoS definitions with 12-row LINEROW entries. This could affect your ability to optimally use native ATM connections among the nodes in your network. Consult technical representatives for the HPR APPN products in your network to determine if those products support CoS definitions with 12-row LINEROW entries.

If you use CoS definitions with 12-row LINEROW entries, routes selected for nonnative ATM sessions could be different than those selected when you use CoS definitions with 8-row LINEROW entries.

The IBM-supplied TG profiles are in IBMTGPS in ASAMPLIB. IBMTGPS is not required, but it is strongly recommended that you include it.

Notes:

1. Because CP-CP session paths may 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.

To prepare the SYS1.VTAMLIB data set, do the following:

1. Allocate the SYS1.VTAMLIB data set using the IEHPROGM utility program, and catalog the data set before SMP/E installation.
2. Define the data set on a direct-access volume (which can be the system residence volume), and secondary space can be allocated. Space requirements are described in the *z/OS Program Directory* that is shipped with the z/OS Communications Server distribution tape.

   SYS1.VTAMLIB is used to store the following 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
3. Code the DD name for SYS1.VTAMLIB as VTAMLIB. You should specify the following 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=
   ```
4. 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 the following format:

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

       FIXED MAX(maxfixK|M)

       ECSA MAX(maxecsaK|M)

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

Notes:

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.

The following describes the variable fields in the CSM parmlib member:

maxfix A decimal integer specifying the maximum bytes of fixed storage to be dedicated for use by CSM. The range is from 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.

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	**4K**	**16K**	**32K**	**60K**	**180K**
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. For more information about this function, refer to *z/OS Communications Server: SNA Network Implementation Guide*.

APPN checkpointing data sets

The following 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:

- Have been the target of a search
- Have a dynamic entry type that is not registered
- Have been 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 V1R6 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 the following:

- 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 the following DCB subparameters for SYS1.DSDB1, SYS1.DSDB2, and SYS1.TRSDB:

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

- Specify the following DCB subparameters for SYS1.DSDBCTRL:

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

Notes:

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

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

Configuration restart data sets

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

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

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.

   The following 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 above.) 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. For a full description of this support, refer to *z/OS Communications Server: SNA Network Implementation Guide*.

To prepare your system to support dynamic configuration of channel-attached devices, complete the following 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 (FFST)

First Failure Support Technology™ 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. For more information on how NODELST is used, refer to *z/OS Communications Server: SNA Network Implementation Guide*.

To define a NODELST data set, perform the following 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.

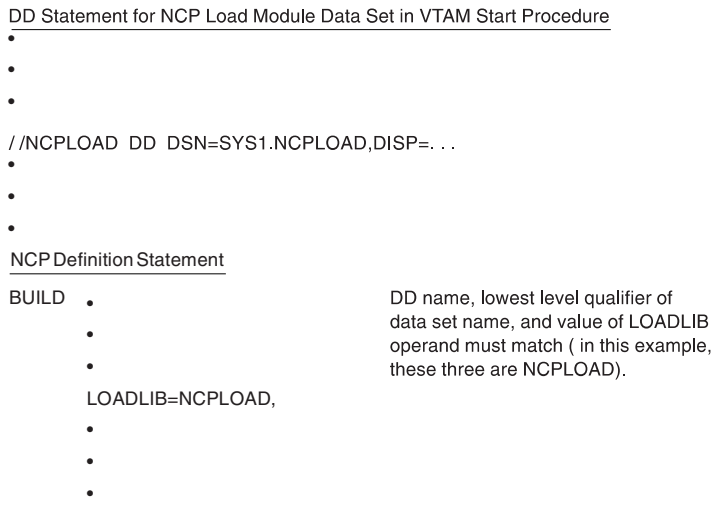

Figure 1. Correlation between DD statement and NCP definition statement

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 the following:

- 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 21 for information on SYS1.SSPLIB requirements.

For more information about the NCP dump data set, refer to 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.

Refer to *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.

Part 2. IP functions

Chapter 2. Roadmap to IP functions

This chapter includes a table designed to be used as a roadmap to the IP functions and enhancements that were introduced in z/OS V1R6 Communications Server, z/OS V1R5 Communications Server, and z/OS V1R4 Communications Server.

The **Enabling / migration actions** column indicates if tasks are required to either utilize the functional enhancement or to satisfy incompatibilities or dependencies. The **Reference** column points you to the section of this document that describes the function.

Table 8. Roadmap to IP functions

Functional enhancement	Enabling / migration actions	Reference
Enhancements introduced in z/OS V1R6 Communications Server		
Policy Agent enhancements	Yes	Page 29
IPv6 support for sysplex enhancements	Yes	Page 30
IPv4 sysplex enhancements for TCPSTACKSOURCEVIPA	No	Page 32
Sysplex profile processing enhancement	Yes	Page 32
Sysplex Distributor and Dynamic VIPA IP forwarding	No	Page 33
Sysplex autonomics	Yes	Page 33
IP packet trace formatting enhancements	Yes	Page 37
IPv6 OSPF support for OMPROUTE	Yes	Page 37
IPv6 support for SNMP TCP/IP subagent	Yes	Page 41
Removal of SMIv1 version of SNMP IBM MVS TCP/IP Enterprise-specific MIB	No	Page 43
TN3270E server address space option	Yes	Page 43
Telnet SCS message table support	Yes	Page 45
FTP Callable API	Yes	Page 46
FTP multi-byte character support	Yes	Page 47
Netstat enhancements	Yes	Page 51
Job specific source IP addressing	Yes	Page 53
Socket option access control	Yes	Page 54
Trivial FTP Daemon (TFTPD) specific bind	Yes	Page 55
Multilevel security enhancements	Yes	Page 56
Support 64-bit virtual addresses for X Windows and Motif	Yes	Page 59
SYNAD exit for SMTP	Yes	Page 61
SYSTCPDA packet trace formatting	Yes	Page 61
Enhancements introduced in z/OS V1R5 Communications Server		
Full Virtual LAN support for OSA-Express	Yes	Page 64
Enterprise Extender enhancements	No	Page 65
Sysplex enhancements	Yes	Page 66
Sysplex Distributor round-robin distribution	No	Page 66

Table 8. Roadmap to IP functions (continued)

Functional enhancement	Enabling / migration actions	Reference
Workload distribution (Application Server Affinity) enhancements	Yes	Page 67
VIPABACKUP enhancement	Yes	Page 69
Dynamically assign Sysplex Distributor ports	Yes	Page 70
DVIPA limit increase	Yes	Page 71
Sysplexports performance enhancement	No	Page 71
Integrated WLM/QoS Performance Monitor	Yes	Page 72
Increase maximum number of allowed sockets	Yes	Page 73
MVS system symbol resolution enhancements in TCPIP.DATA	Yes	Page 74
Netstat enhancements	Yes	Page 74
Intrusion Detection Services enhancements	Yes	Page 76
Multilevel security	Yes	Page 77
OMPROUTE enhancements	Yes	Page 78
TCP/IP asynchronous I/O support enhancements	Yes	Page 81
Policy code restructure	Yes	Page 82
Managed System Infrastructure (msys) for Setup FTP customization support	Yes	Page 83
MVS Remote Execution Server support for multilevel security	Yes	Page 83
OSA performance enhancements	Yes	Page 84
Improve diagnostics for DLC dumps	No	Page 85
DHCP daemon enhancement	Yes	Page 85
CTRACE formatting filter enhancements	Yes	Page 86
SMTP support for IP Mailer Name	Yes	Page 86
HiperSockets broadcast support	Yes	Page 87
Network management	Yes	Page 87
Exploitation of IBM CP assist for cryptographic functions	No	Page 89
IBM @server zSeries 990 HiperSockets enhancements	No	Page 90
IPv6 support — Full Virtual LAN (VLAN) support for OSA-Express	Yes	Page 92
IPv6 support for Enterprise Extender	No	Page 93
IPv6 support and upgrade for Sendmail	Yes	Page 93
IPv6 support for CICS sockets API	Yes	Page 98
IPv6 support for Policy	Yes	Page 101
IPv6 support for the SYSLOG daemon and the DCAS, TFTP, and SNTP servers	Yes	Page 102
IPv6 support for TSO rexec and rsh and associated MVS daemons	Yes	Page 103
IPv6 support for SMF recording	Yes	Page 104
IPv6 support enhancements for Netstat	Yes	Page 107
IPv6 support for XCF, SameHost, and ESCON	Yes	Page 105
IPv6 support enhancement for IPAQENET6 Interface type	Yes	Page 106

Table 8. Roadmap to IP functions (continued)

Functional enhancement	Enabling / migration actions	Reference
IPv6 support for dynamic XCF	Yes	Page 106
IPv6 support enhancements for OMPROUTE	Yes	Page 108
IPv6 support for network access control	Yes	Page 110
Autoconfigure target library for FTP load module transfer	Yes	Page 111
Define FTP ephemeral port range for firewall compatibility	Yes	Page 113
FTP TLS support enhancements	Yes	Page 114
Improve FTP serviceability	Yes	Page 115
Enforce nonzero error return code in FTP	Yes	Page 117
Allow the FTP server load module to run above the 16M line	Yes	Page 118
Display status of FTPKEEPALIVE timer	Yes	Page 119
FTP SERVAUTH Port of Entry support	Yes	Page 120
TN3270 IP address range configuration	Yes	Page 121
TN3270 Takeover enhancement	Yes	Page 121
TN3270 keyboard control enhancements	Yes	Page 122
IPv6 support for TN3270	Yes	Page 122
TN3270 Network Management	Yes	Page 123
Improve performance for TN3270 definite response sessions	No	Page 124
Network Access Control for TN3270	Yes	Page 124
Multilevel security LU name assignment support for TN3270	Yes	Page 125
IPv6 support for SNMP applications	Yes	Page 126
SNMP TCP/IP subagent	Yes	Page 127
SNMP Network SLAPM2 subagent	Yes	Page 129
SNMP TN3270 Telnet subagent	Yes	Page 130
Enhancements introduced in z/OS V1R4 Communications Server		
Sysplex-wide Dynamic Source VIPAs for TCP connections	Yes	Page 134
Sysplexports	Yes	Page 135
Sysplex Wide Security Association (SWSA)	Yes	Page 136
Network access control	Yes	Page 137
Fast Response Cache Accelerator (FRCA) access control	Yes	Page 138
Resolver enhancements (general enhancement — see page 151 for resolver enhancements related to IPv6 support)	Yes	Page 139
Managed System Infrastructure (msys) for Setup enhancement	Yes	Page 140
OSA-Express Direct SNMP subagent support	No	Page 140
Event trace enhancements	Yes	Page 141
TCP/IP support for Simple Network Time Protocol (SNTP)	Yes	Page 142
Netstat enhancements (general enhancement — see page 153 for Netstat enhancements related to IPv6 support)	No	Page 143
Ping enhancements (general enhancement — see page 154 for Ping enhancements related to IPv6 support)	Yes	Page 143
Traceroute enhancements (general enhancement — see page 154 for Traceroute enhancements related to IPv6 support)	Yes	Page 143

Table 8. Roadmap to IP functions (continued)

Functional enhancement	Enabling / migration actions	Reference
New VTAM start options to adjust the QDIO or iQDIO storage	Yes	Page 147
Enabling IPv6 support	Yes	Page 148
Configuration changes related to IPv6 support	Yes	Page 149
IPv6 support for the resolver	Yes	Page 151
IPv6 support for applications	Yes	Page 152
IPv6 support for Netstat	Yes	Page 153
IPv6 support for Ping	Yes	Page 154
IPv6 support for Traceroute	Yes	Page 154
IPv6 support for IPv6 IPCS subcommands formatting	No	Page 155
IPv6 support for event trace enhancements	Yes	Page 155
IPv6 support for RAS packet trace and data trace	No	Page 156
IPv6 support for socket API commands	Yes	Page 156
FTP support for substitution characters during EBCDIC/ASCII single-byte translations	Yes	Page 157
FTP: Enhanced FTP activity logging	Yes	Page 158
FTP: Changed behavior of login failure replies	No	Page 158
FTP: Support for Chinese standard GB18030 provided by codepage IBM-5488	Yes	Page 159
FTP: Enhancements to FTP server user exits	Yes	Page 160
FTP: IPv6 support for FTP	Yes	Page 162
Telnet: Port qualification by linkname or destination IP address	Yes	Page 163
Telnet: Printer enhancements	Yes	Page 164
Telnet: Parameter placement enhancements	No	Page 165
Telnet: New DEBUG option to suppress the connection dropped error messages	Yes	Page 165
Telnet: New QINIT option for default applications	Yes	Page 166
Telnet: LU mapping enhancements	Yes	Page 167
Upgrade TN3270 SSL to use TLS	No	Page 168
DNS enhancements, including IPv6 support	Yes	Page 169

Chapter 3. V1R6 IP new function summary

This chapter includes a section for every function or enhancement introduced for IP in z/OS V1R6 Communications Server. The sections include the following 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.

See Table 8 on page 25 for a complete list of the IP functional enhancements of the current and recent releases.

Refer to *z/OS Migration* for information about how to maintain the functional behavior of previous releases. Refer to *z/OS Summary of Message and Interface Changes* for information on new and changed messages and interfaces.

General considerations

In addition to the function-specific tasks of this chapter, be aware of the following general considerations:

- In order to allow OMPROUTE wildcarding to work properly, DEVICE, LINK, and INTERFACE names should not contain an asterisk (*).

Policy Agent enhancements

The Policy Agent API (PAPI) is enhanced with two additional functions used to access policy performance data. These functions allow an application to access performance data by policy rule or policy action ID instead of sequentially accessing all policy rules or policy actions. In addition, the Policy Agent PEPInstance configuration statement is added as a synonym for the existing TcpImage statement. Some implementations of Policy Agent may use the PEPInstance statement; therefore, this change allows for configurations to be common among different implementations.

Restrictions

None.

What this change affects

- Customization
- Application Development

Using this function

If you want to use the Policy Agent enhancements, perform the task in the following table. Refer to Helper functions in the Policy API (PAPI) chapter in *z/OS Communications Server: IP Programmer's Reference* for more information.

Table 9. Policy Agent enhancements

Task	Procedure
Change or write Policy Agent applications using the PAPI interface to take advantage of new PAPI functions.	Use the papi_get_rule_perf_by_id() or papi_get_action_perf_by_id() functions as an alternative to papi_get_rule_perf_info() or papi_get_action_perf_info() to access policy performance data.

Sysplex enhancements

In z/OS V1R6 Communications Server, sysplex is enhanced in the following areas:

- "IPv6 support for sysplex enhancements"
- "IPv4 sysplex enhancements for TCPSTACKSOURCEVIPA" on page 32
- "Sysplex profile processing enhancement" on page 32
- "Sysplex Distributor and Dynamic VIPA IP forwarding" on page 33
- "Sysplex autonomics" on page 33

IPv6 support for sysplex enhancements

Changes in regard to IPv6 support for sysplex were made in z/OS V1R6 Communications Server in the following areas:

- TCP/IP sysplex functions now support IPv6.

  If you are deploying IPv6 applications, you will be able to take advantage of the availability and workload balancing capabilities of z/OS TCP sysplex functions for your mission-critical IPv6 applications, as you have been able to do in past releases for IPv4 applications. Refer to the discussion on IPv6 special considerations in *z/OS Communications Server: IP Configuration Guide* for more information.

  In addition, the Policy Agent is changed to support IPv6 addresses for the Policy Agent to Policy Agent connections that are established for the Sysplex Distributor Performance Monitoring function.
- The netstat,config display for the IPv4 section will now display either a subnet or the num_mask_bits with the DYNAMICXCF address, depending on how it was configured.

Restrictions

V1R6 does not provide IPv6 support for the following IPv4 sysplex functions:

- Sysplex Wide Security Associations (SWSA)
- Sysplex Distributor Integration with Cisco MNLB
- MOVEABLE WHENIDLE and MOVEABLE DISRUPTIVE
- HiperSockets™ connectivity

The types of addresses allowed for the TCPSTACKSOURCEVIPA configuration option are restricted to the following:

- Static VIPAs
- Active Dynamic VIPAs

Dependencies

IPv6 must be enabled in the TCP/IP stack.

Coexistence requirements

All stacks (routing stack, backup stack, target stack) which participate in distribution for an IPv6 Distributed DVIPA must be running on z/OS V1R6 or higher and have IPv6 enabled.

What this change affects

- Application development
- Availability
- Operations
- Customization

Using this function

If you want to use the IPv6 support for sysplex enhancements, perform the desired tasks in the following table.

Table 10. IPv6 support for sysplex enhancements

Task	Procedure	Reference
Exploit the So_Clusterconntype option of getsockopt().	Issue the SO_CLUSTERCONNTYPE getsockopt() on the IPv6 socket.	getsockopt() in *z/OS Communications Server: IP Application Programming Interface Guide*
Enable source VIPA for IPv6 Dynamic XCF.	On the IPCONFIG6 statement, code DYNAMICXCF SOURCEVIPAINT specifying an interface.	Connectivity in a sysplex in *z/OS Communications Server: IP Configuration Guide* and IPCONFIG6 statement in *z/OS Communications Server: IP Configuration Reference*
Define IPv6 Dynamic VIPAs.	Within the VIPADYNAMIC/ENDVIPADYNAMIC block, code a VIPADEFINE statement to define the IPv6 interface and its associated IPv6 DVIPA.	Virtual IP addressing in *z/OS Communications Server: IP Configuration Guide* and VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*
Define backup stacks for the defined IPv6 Dynamic VIPAs.	For each stack that will act as a backup, code a VIPABACKUP statement with the IPv6 interface and associated IPv6 DVIPA of the IPv6 DVIPAs being backed up. Do this within the VIPADYNAMIC/ENDVIPADYNAMIC block.	Virtual IP addressing in *z/OS Communications Server: IP Configuration Guide* and VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*
Define a range of potential IPv6 Dynamic VIPAs on a stack within the Sysplex.	Code a VIPARANGE statement with an IPv6 interface and its associated IPv6 address and prefixlength. Do this within the VIPADYNAMIC/ENDVIPADYNAMIC block.	Virtual IP addressing in *z/OS Communications Server: IP Configuration Guide* and VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*
Cause a defined IPv6 Dynamic VIPA to be distributed to other stacks within the Sysplex.	Within the VIPADYNAMIC/ENDVIPADYNAMIC block for each routing stack, code a VIPADISTRIBUTE statement specifying the dynamic XCF addresses of the target stacks within the Sysplex to which a DVIPA should be distributed.	Virtual IP addressing in *z/OS Communications Server: IP Configuration Guide* and VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*

Table 10. IPv6 support for sysplex enhancements (continued)

Task	Procedure	Reference
Define an IPv6 TCP stack source VIPA for connections using IPv6 routes.	On the IPCONFIG6 statement, code SOURCEVIPA and TCPSTACKSOURCEVIPA specifying an IPv6 interface name of a static or dynamic VIPA.	Virtual IP addressing in *z/OS Communications Server: IP Configuration Guide* and IPCONFIG6 statement in *z/OS Communications Server: IP Configuration Reference*
Modify Policy Configuration file, PolicyAction statement OutboundInterface, to include IPv6 addresses.	Specify an IPv6 outbound interface for the Sysplex Distributor distributing stack.	Quality of Service in *z/OS Communications Server: IP Configuration Guide* and POLICYACTION statement in *z/OS Communications Server: IP Configuration Reference*
Allow an IPv6 DVIPA to be activated on a backup TCP/IP before it has been activated on the TCP/IP where it is defined with VIPADEFINE.	Do the following: • Add MOVEABLE IMMEDIATE to the VIPABACKUP statement for the IPv6 DVIPA. • Start the backup TCP/IP stack with the updated VIPABACKUP statement in the initial profile, or issue the VARY TCPIP,,OBEYFILE command on the backup TCP/IP stack referencing the data set that contains the updated VIPABACKUP statement.	Configuring VIPAs for activation with VIPABACKUP in *z/OS Communications Server: IP Configuration Guide* and VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*
When using VIPARANGE, control which applications may bind() to create a DVIPA.	Define a RACF profile EZB.BINDDVIPARANGE.sysname.tcpname in the SERVAUTH class and permit the applications. If the profile is not defined, no checking is performed. Non-IBM security products may require the profile to be defined and applications to be permitted.	Defining a RACF profile for VIPARANGE in *z/OS Communications Server: IP Configuration Guide*

IPv4 sysplex enhancements for TCPSTACKSOURCEVIPA

For sysplex-wide dynamic source VIPAs for TCP connections, the types of addresses allowed for the TCPSTACKSOURCEVIPA configuration option is restricted to the following:

- Static VIPAs
- Active dynamic VIPAs

Sysplex profile processing enhancement

The processing of VIPADYNAMIC statements is changed to work the same whether the statements were specified within a single profile or within separate profiles. In previous releases, if a Dynamic Virtual IP Address (DVIPA) was specified in more than one VIPADEFINE or VIPABACKUP statement within a single profile, only the last VIPADEFINE or VIPABACKUP statement containing the DVIPA would be processed. Now, all statements within a single profile will be processed.

Restrictions

This change only affects VIPADEFINE, VIPABACKUP and VIPADELETE statements.

Incompatibilities

If there are VIPADEFINE or VIPABACKUP statements in your TCPIP profile which contain duplicate Dynamic Virtual IP Addresses (DVIPA), you may need to change your profile.

What this change affects

- Customization

Using this function

Because of the sysplex profile processing enhancement, you may need to perform the task in the following table.

Table 11. Sysplex profile processing enhancement

Task	Procedure	Reference
Change your profile if your TCPIP profile has multiple VIPADEFINE or VIPABACKUP statements for the same dynamic VIPA address (DVIPA).	Edit your profile and do one of the following: • **Guideline:** Remove all VIPADEFINES and VIPABACKUPs for the same dynamic VIPA address so that only the one, desired definition remains. • Place a VIPADELETE statement before the last VIPADEFINE or VIPABACKUP statement.	VIPADYNAMIC statement in *z/OS Communications Server: IP Configuration Reference*

Sysplex Distributor and Dynamic VIPA IP forwarding

In prior releases, the TCP/IP stack that was configured as a distributor of dynamic VIPAs was required to enable IP forwarding using the IPCONFIG DATAGRAMFWD TCP/IP profile statement. For installations that do not wish to configure their TCP/IP stack as a forwarding node, it is no longer a requirement for distributing dynamic VIPAs. However, if your installation is configured such that target TCP/IP stacks only have XCF connectivity, datagram forwarding still needs to be configured on the distributor, as all packets originating from the target will be forwarded by the distributor.

Sysplex autonomics

There are two areas that are enhanced in z/OS V1R6 Communications Server for sysplex autonomics:

- Automated recovery
- Planned takeback

Automated recovery enhancements

TCP/IP sysplex-related functions are enhanced to provide additional autonomic features that improve the availability attributes of configurations that are exploiting Dynamic Virtual IP Address (DVIPA) technologies in a z/OS sysplex environment. Users that currently exploit DVIPA support in a sysplex environment should carefully review and evaluate these new functions.

DVIPA and distributed DVIPA functions allow users to leverage their sysplex environments by providing high availability TCP/IP communications to applications running in a sysplex environment, even when failures of individual components occur. For example, the Sysplex Distributor function, which relies on distributed DVIPA technology, can be used to allow for load balancing of incoming TCP connections to a cluster of application servers residing inside the sysplex. Sysplex Distributor TCP connection load balancing offers performance benefits by routing connections to multiple servers versus a single server, and also minimizes

the impact of a failure of a critical resource by rerouting connection requests around the failing component. For example, prior to z/OS V1R6, the following failures can be detected automatically:

- When an MVS operating system instance within the sysplex fails, it can be removed from the sysplex automatically if a Sysplex Failure Management (SFM) policy or equivalent automation has been set up, or manually by responding to the console WTOR message that indicates the failure and indicating that the system should be removed from the sysplex. In either case, once the system is removed from the sysplex, all TCP/IP stacks instances in the remaining systems in the sysplex will automatically perform any necessary cleanup and recovery actions. This includes performing any DVIPA Takeover processing necessary for any DVIPAs owned by the failing system and removing the failing system from the candidate target list for any distributed DVIPAs that listed the failing system as an eligible target.
- When a TCP/IP stack instance fails (such as when the TCP/IP address space is terminated) or is terminated normally, the remaining TCP/IP stack instances in the sysplex are immediately notified of the event and proceed to perform automated recovery actions (DVIPA Takeover activities described in the previous scenario).
- When a specific application address space that is associated with a DVIPA terminates, several automated recovery actions can take place. If the application instance was an eligible target for a distributed DVIPA, it is removed from the target list for this DVIPA by the Sysplex Distributor primary routing stack. If the application was associated with a Unique Application-Instance DVIPA, user provided automation, such as an Automatic Restart Manager (ARM) policy or an Automation product, can restart the application on the same system or another system in the sysplex, automatically triggering the movement of the Unique Application-Instance DVIPA.

The new sysplex problem autonomics functions introduced in this release complement these existing functions by adding comprehensive self-monitoring processing that allows each TCP/IP stack instance that is a member of the TCP/IP XCF group (EZBTCPCS group) to detect severe shortages of key resources or failure of key components on the local system that are required for proper operation of DVIPA functions in a sysplex environment. When a TCP/IP stack instance detects these conditions and determines that it can no longer function properly as a member of the TCP/IP sysplex group (for example, as a Sysplex Distributor Primary/Backup Router, as a distributed DVIPA Target system or as an owner/backup of a DVIPA) it may automatically remove itself from the TCP/IP XCF group. This will allow other systems in the sysplex to perform any automated recovery actions necessary (DVIPA Takeover activities described above).

Note that these sysplex self-monitoring functions will be activated automatically when TCP/IP joins its XCF group during initialization and cannot be disabled. As a result, if these functions detect a problem condition, new messages will be issued to the console. The automated recovery processing (such as the local TCP/IP stack leaving the TCP/IP sysplex group) is disabled by default when a TCP/IP stack joins the TCP/IP XCF group during initialization. It is recommended that you enable the automated recovery by using the new configuration parameter, SYSPLEXMONITOR, which has been added to the GLOBALCONFIG statement in the TCPIP profile. It allows users to control whether the automated recovery processing should be activated or not, and to also specify how responsive the monitoring and recovery processing should be (such as how long the problem conditions must persist before an alert is generated and any applicable recovery actions are taken).

When this function is enabled, it provides for automated recovery actions that can help limit the impact of a failure within a single TCP/IP stack instance or system. For example, if a problem occurs within a Sysplex Distributor primary routing stack that prevents it from functioning properly, it may manifest itself as a sysplex-wide outage for the workloads dependent on the distributed DVIPAs that are owned by this stack. This can be avoided by initiating an automated recovery action that allows the backup TCP/IP stacks for these distributed DVIPAs to perform a takeover for the distribution role.

While having these automated recovery actions active should be desirable for most users, it is important to understand the conditions that are monitored and that could potentially trigger the automated recovery actions so that you can properly plan any operational changes required and to determine the settings for this function that are appropriate in your environment. For example, one of the monitoring functions involves checking whether the VTAM address space is active or not. If VTAM is found to be inactive for a time period (60 seconds by default or by the specified timer interval on the SYSPLEXMONITOR parameter) the local TCP/IP stack will issue an eventual action message and leave the TCP/IP sysplex group. As a result, caution should be taken when stopping VTAM for extended periods of time while TCP/IP is active, as the automated recovery actions may be triggered.

When the TCP/IP stack leaves the TCP/IP sysplex group, it will delete all local DVIPA configuration information and stop advertising routes (using the dynamic routing protocols that have been configured) for any of the DVIPAs that it currently owns. The local TCP/IP stack can rejoin the TCP/IP sysplex group by way of manual intervention once the condition that caused the automated recovery action to take place has been relieved (for example, for the scenario above, VTAM is now active). This can be achieved by issuing a VARY TCPIP,,OBEYFILE operator command with a data set that includes all the VIPADYNAMIC block definitions, or (for example, in the case of a pure target stack) an IPCONFIG(6) DYNAMICXCF statement, or by recycling the local TCP/IP stack.

In addition, a new operator command has been provided to allow users to force a local TCP/IP stack to leave the TCP/IP sysplex group.

For more details on these self-monitoring and automated recovery functions, refer to Sysplex problem detection and recovery in *z/OS Communications Server: IP Configuration Guide*.

Planned takeback enhancement

TCP/IP sysplex-related functions were enhanced to provide additional startup features that improve the availability of TCP/IP sysplex functions during a planned takeback. Users that currently exploit DVIPA support in a sysplex environment should carefully review and evaluate this new function.

During a planned or unplanned outage, the dynamic VIPAs and/or distributable VIPAs for a TCP/IP stack are taken over by backup TCP/IP stack(s). When the primary TCP/IP stack is restarted, the dynamic VIPAs and/or distributable VIPAs are taken back from the backup TCP/IP stack(s). If dynamic routing is used to notify others of these VIPAs, and OMPROUTE is not yet active on the primary TCP/IP stack, existing connections to these VIPAs may be reset and new connect requests to these VIPAs may fail. By using the GLOBALCONFIG SYSPLEXMONITOR DELAYJOIN configuration statement in the TCP/IP profile on the primary TCP/IP stack, it is possible to delay taking back the dynamic VIPAs and/or distributable VIPAs until OMPROUTE is started and active. Thus, new and

existing connections will continue to be serviced by the backup TCP/IP stacks until OMPROUTE is active on the primary TCP/IP stack. For more details about the GLOBALCONFIG statement, refer to GLOBALCONFIG statement in *z/OS Communications Server: IP Configuration Reference* .

Restrictions

None.

What this change affects

- Availability
- Diagnosis
- Operations

Using this function

If you want to use sysplex autonomics, perform the desired tasks in the following table.

Table 12. Sysplex autonomics

Task	Procedure	Reference
Enable sysplex autonomics function.	Code SYSPLEXMONITOR RECOVERY on the GLOBALCONFIG statement; this function is enabled when the member joins the TCP/IP sysplex group (EZBTCPCS). **Guideline:** Enable this function.	Sysplex problem detection and recovery in *z/OS Communications Server: IP Configuration Guide* and GLOBALCONFIG statement in *z/OS Communications Server: IP Configuration Reference*
Check and update the WLM service classes for TCP and OMPROUTE.	Ensure that the TCP/IP and OMPROUTE address spaces are placed in the SYSSTC service classification.	Sysplex problem detection and recovery in *z/OS Communications Server: IP Configuration Guide*
Disable the sysplex autonomics function.	This function is disabled by default. If you previously enabled it and now want to disable it, code SYSPLEXMONITOR NORECOVERY on the GLOBALCONFIG statement.	Sysplex problem detection and recovery in *z/OS Communications Server: IP Configuration Guide* and GLOBALCONFIG statement in *z/OS Communications Server: IP Configuration Reference*
Resolve detected sysplex problems.	Follow instructions within error messages that display the cause of the problem and the remedy.	*z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)*
Remove a member from the TCP/IP sysplex group because it is no longer functioning correctly (for example, a routing node that is no longer distributing new connections or a target stack that is timing out during new connection establishment to a DVIPA application).	Issue the leave group command: VARY TCPIP,,SYSPLEX,LEAVEGROUP This will cause the member to remove all sysplex configuration information.	VARY TCPIP,,SYSPLEX in *z/OS Communications Server: IP System Administrator's Commands*
Ensure you have operational/recovery procedures in place to enable any stack in the sysplex to rejoin the TCP/IP sysplex group after a problem has been detected.	The original sysplex configuration information will need to be reapplied using a VARY TCPIP,,OBEYFILE command. Variation in the sysplex configuration information will automatically cause the member to rejoin the TCP/IP Sysplex group.	Sysplex problem detection and recovery in *z/OS Communications Server: IP Configuration Guide* and VARY TCPIP,,OBEYFILE in *z/OS Communications Server: IP System Administrator's Commands*

Table 12. Sysplex autonomics (continued)

Task	Procedure	Reference
Delay joining or rejoining the TCP/IP sysplex group until after OMPROUTE has been started.	Code the SYSPLEXMONITOR DELAYJOIN keyword on the GLOBALCONFIG statement.	GLOBALCONFIG statement in *z/OS Communications Server: IP Configuration Reference*

IP packet trace formatting enhancements

z/OS V1R6 Communications Server enhances the formatting of TCP/IP packet traces in the following ways:

- The packet traces include Enterprise Extender packets that flow to and from TCP/IP. Prior to z/OS V1R6 Communications Server, Enterprise Extender packets could only be dumped.
- The formatting verifies the checksum of the selected packets.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

If you want to use the packet trace formatting enhancements, perform the tasks in the following table.

Table 13. IP packet trace formatting enhancements

Task	Procedure	Reference
Start Enterprise Extender packet traces.	Issue VARY TCPIP,,PKTTRACE,DESTP=12000 and VARY TCPIP,,PKTTRACE,SRCP=12000. Repeat for ports 12001 through 12004.	VARY TCPIP,,PKTTRACE in *z/OS Communications Server: IP System Administrator's Commands*
Format Enterprise Extender packet traces.	Issue using IPCS: CTRACE COMP(SYSTCPDA) OPTIONS((EE FORMAT)).	Packet trace (SYSTCPDA) for TCP/IP stacks in *z/OS Communications Server: IP Diagnosis Guide*
Start packet traces for checksum verification.	Issue VARY TCPIP,,PKTTRACE,[selection parameters].	VARY TCPIP,,PKTTRACE in *z/OS Communications Server: IP System Administrator's Commands*
Format packet traces for checksum verification.	Issue using IPCS: CTRACE COMP(SYSTCPDA) OPTIONS((CHECKSUM(DETAIL))).	Packet trace (SYSTCPDA) for TCP/IP stacks in *z/OS Communications Server: IP Diagnosis Guide*

IPv6 OSPF support for OMPROUTE

z/OS V1R6 Communications Server adds OMPROUTE support for the IPv6 OSPF dynamic routing protocol. This support enables OSPF dynamic routing over IPv6, resulting in quicker convergence of network changes than offered by IPv6 RIP. OSPF also works together with VIPA and Sysplex to enhance availability of z/OS and the resources it provides and uses in the network.

Restrictions

The following restrictions apply:

- Not-so-stubby area (NSSA) is not supported for IPv6 OSPF.
- OMPROUTE does not support multiple instances of IPv6 OSPF on a single link.
- Each IPv6 OSPF interface can only have one instance number.
- In V1R6, the z/OS TCP/IP stack does not include support for IPv6 IPSec. Because of this, it is not possible to use IPSec to authenticate IPv6 OSPF routing exchanges on any link over which OMPROUTE establishes adjacencies. IPv6 OSPF may be used but IPSec will not be present.

Dependencies

IPv6 must be enabled in the TCP/IP stack.

What this change affects

- Availability
- Operations
- Storage
- Customization

Using this function

If you want to use the IPv6 OSPF support for OMPROUTE, perform the desired tasks in the following table.

Refer to Steps for configuring OSPF and RIP (IPv4 and IPv6) in *z/OS Communications Server: IP Configuration Guide* for more information.

Table 14. IPv6 OSPF support for OMPROUTE

Task	Procedure	Reference
Enable IPv6 dynamic routing using IPv6 OSPF.	Define IPv6 interfaces to OMPROUTE by using IPV6_OSPF_INTERFACE statements for interfaces over which the IPv6 OSPF protocol will run.	IPv6 dynamic routing using OMPROUTE and Define IPv6 interfaces, if the IPv6 OSPF or IPv6 RIP protocol is used in *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Specify prefixes that reside on the link to which an OSPF interface attaches, which will not be advertised to this host by way of router discovery or OSPF.	Define the prefix parameter on the interface's IPV6_OSPF_INTERFACE statements.	*z/OS Communications Server: IP Configuration Reference*
Define wildcard IPv6 OSPF interfaces.	Code IPV6_OSPF_INTERFACE definition statements, using a wildcard interface name ending in *. For example, VIPA* matches all interfaces whose names begin with the characters VIPA.	Define IPv6 interfaces, if the IPv6 OSPF or IPv6 RIP protocol is used in *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Define various parameters that apply globally to IPv6 OSPF.	Code the IPV6_OSPF statement in the OMPROUTE configuration file.	*z/OS Communications Server: IP Configuration Reference*

Table 14. IPv6 OSPF support for OMPROUTE (continued)

Task	Procedure	Reference
Define an IPv6 OSPF area to which a local IPv6 OSPF interface attaches.	Code the IPV6_AREA statement in the OMPROUTE configuration file.	Define OSPF areas, if the OSPF protocol is used in *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Define an IPv6 OSPF totally stubby area.	Code the STUB_AREA=YES and IMPORT_PREFIXES=NO parameters on the area's IPV6_AREA configuration statement.	*z/OS Communications Server: IP Configuration Reference*
Enable IPv6 OSPF AS Boundary Routing capability, allowing routes learned from other methods (such as IPv6 RIP) to be imported into the IPv6 OSPF domain.	Code the IPV6_AS_BOUNDARY_ROUTING statement in the OMPROUTE configuration file.	*z/OS Communications Server: IP Configuration Reference*
Allow a group of routes within an IPv6 OSPF area that share a common prefix to be advertised externally to the area as a single prefix route.	Code the IPV6_RANGE statement with ADVERTISE=YES in the OMPROUTE configuration file.	Limit information exchange between OSPF areas, if the OSPF protocol is used in *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Keep a group of routes within an IPv6 OSPF area that share a common prefix from being advertised externally to the area.	Code the IPV6_RANGE statement with ADVERTISE=NO in the OMPROUTE configuration file.	Limit information exchange between OSPF areas, if the OSPF protocol is used in *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Define a virtual link between two IPv6 OSPF area border routers for the purpose of maintaining backbone connectivity.	Code the IPV6_VIRTUAL_LINK statement in the OMPROUTE configuration file.	Configure virtual links, if the OSPF protocol is used in *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Advertise this router as an IPv6 OSPF default router.	Do one of the following: • Use BEGINROUTES in the TCP/IP profile to define static IPv6 default routes. • Code IPV6_AS_BOUNDARY_ROUTING statement with IMPORT_STATIC_ROUTES=YES in the OMPROUTE configuration file. • Code IPV6_AS_BOUNDARY_ROUTING statement with ORIGINATE_DEFAULT_ROUTE=YES in the OMPROUTE configuration file.	Steps for configuring OMPROUTE in *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Display a comprehensive list of IPv6 OSPF information.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6OSPF,ALL command.	*z/OS Communications Server: IP System Administrator's Commands*
Display statistics and parameters for all IPv6 OSPF areas attached to the router.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6OSPF, AREASUM command.	*z/OS Communications Server: IP System Administrator's Commands*

Table 14. IPv6 OSPF support for OMPROUTE (continued)

Task	Procedure	Reference
Display statistics and parameters related to IPv6 OSPF interfaces.	Use the DISPLAY TCPIP,stackname, OMPROUTE, IPV6OSPF,INTERFACE command to see a summary of all IPv6 OSPF interfaces. To see more detailed information about a specific IPv6 OSPF interface, use the DISPLAY TCPIP,stackname, OMPROUTE, IPV6OSPF,INTERFACE,NAME=if-name command or the DISPLAY TCPIP,stackname, OMPROUTE, IPV6OSPF,INTERFACE,ID=if-id command.	*z/OS Communications Server: IP System Administrator's Commands*
Display statistics and parameters related to IPv6 OSPF virtual links.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6OSPF, VLINK command to see a summary of all IPv6 OSPF virtual links. To see more detailed information about a specific IPv6 OSPF virtual link, use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6OSPF, VLINK, ENDPT=router-id command.	*z/OS Communications Server: IP System Administrator's Commands*
Display statistics and parameters related to IPv6 OSPF neighbors.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6OSPF, NEIGHBOR command to see a summary of all IPv6 OSPF neighbors. To see more detailed information about a specific IPv6 OSPF neighbor, use the DISPLAY TCPIP,stackname, OMPROUTE,IPV6OSPF,NEIGHBOR,ID= router-id command. If the neighbor specified by the ID= parameter has more than one neighbor relationship with OMPROUTE, the IFNAME= parameter can be used to specify which link's adjacency to examine.	*z/OS Communications Server: IP System Administrator's Commands*
Display the number of Link State Advertisements currently in the IPv6 OSPF link state database, categorized by type.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6OSPF, DBSIZE command.	*z/OS Communications Server: IP System Administrator's Commands*
Display the contents of a single link state advertisement in the IPv6 OSPF link state database.	Use the DISPLAY TCPIP,stackname, OMPROUTE,IPV6OSPF,LSA, LSTYPE=ls-type, LSID=lsid,ORIG=ad-router,AREAID=area-id command. Each interface has its own set of link LSAs. IFNAME=interface_name on the command line indicates which links LSA you want to display.	*z/OS Communications Server: IP System Administrator's Commands*
Display the AS external advertisements belonging to the IPv6 OSPF routing domain.	Use the DISPLAY TCPIP,stackname, OMPROUTE,IPV6OSPF,EXTERNAL command.	*z/OS Communications Server: IP System Administrator's Commands*
Display the contents of a particular IPv6 OSPF area link state database.	Use the DISPLAY TCPIP,stackname, OMPROUTE,IPV6OSPF, DATABASE,AREAID=area-id command.	*z/OS Communications Server: IP System Administrator's Commands*

Table 14. IPv6 OSPF support for OMPROUTE (continued)

Task	Procedure	Reference
Display routes to all other routers that have been calculated by IPv6 OSPF and are now present in the routing table.	Use the DISPLAY TCPIP,stackname, OMPROUTE,IPV6OSPF,ROUTERS command.	*z/OS Communications Server: IP System Administrator's Commands*
Display statistics generated by the IPv6 OSPF routing protocol.	Use the DISPLAY TCPIP,stackname, OMPROUTE,IPV6OSPF,STATISTICS command.	*z/OS Communications Server: IP System Administrator's Commands*
Set the MTU value for IPv6 OSPF interfaces.	Code the MTU value on the INTERFACE statement in TCP/IP profile. OMPROUTE will learn this value from TCP/IP. It is not necessary to code MTU values in OMPROUTE for IPv6 interfaces.	*z/OS Communications Server: IP Configuration Reference*
Dynamically change the cost of an IPv6 OSPF interface.	Use the MODIFY procname,IPV6OSPF,WEIGHT,NAME=name, COST=cost command, specifying the name of the interface and the new cost value.	*z/OS Communications Server: IP System Administrator's Commands* and Changing the cost of OSPF links in *z/OS Communications Server: IP Configuration Guide*
Format IPv6 OSPF packet trace.	Issue using IPCS: CTRACE COMP(SYSTCPDA) OPTIONS((OSPF FORMAT)).	Packet trace (SYSTCPDA) for TCP/IP stacks in *z/OS Communications Server: IP Diagnosis Guide*

IPv6 support for SNMP TCP/IP subagent

The following changes were made for the SNMP TCP/IP subagent:

- Added additional support for IPv6 MIB data. The IPv6 MIB data is supported in version-neutral MIB objects. Version-neutral MIB objects can support both IPv4 and IPv6 processing. In V1R6, the TCP/IP subagent was enhanced to support changed or additional version-neutral standard MIB data from the following IETF Internet drafts:
  - IP-MIB from draft-ietf-ipv6-rfc2011-update-04.txt
  - IP-FORWARD-MIB from draft-ietf-ipv6-rfc2096-update-05.txt
  - TCP-MIB from draft-ietf-ipv6-rfc2012-update-04.txt

  Since IETF internet drafts expire in 6 months, copies of these versions of the internet drafts are shipped with z/OS CS V1R6 and installed in the HFS in the /usr/lpp/tcpip/samples directory with the following file names:
  - ipmib.mi2 - IP-MIB
  - ipfwdmib.mi2 - IP-FORWARD-MIB
  - tcpmib.mi2 - TCP-MIB
  - iaddrmib.mi2 - INET-ADDRESS-MIB. This file is the INET-ADDRESS-MIB from draft-ietf-ops-rfc3291bis-01.txt. The INET-ADDRESS-MIB contains SNMP MIB data textual conventions referenced by MIB data definitions in the standard MIB modules.
- Added additional support for IPv6 MIB data in the IBM MVS TCP/IP Enterprise-specific MIB in the areas of:
  - Added support for IPv6 dynamic VIPA information.
    - Support for the following MIB data was enhanced to provide IPv6 dynamic VIPA information:
      - ibmMvsDVIPATable

- ibmMvsDVIPADistConfTable
- ibmMvsDVIPAConnRoutingTable
- ibmMvsDVIPADistPortTable
- dynamic VIPA traps

- Added new MIB table, ibmMvsDVIPARangeConfigTable, which supports both IPv4 and IPv6 information.
- Deprecated the ibmMvsDVIPARangeConfTable since it can only support IPv4 information. This table will continue to be supported but will only provide information for IPv4 dynamic VIPAs.

– remote ping — Added ibmRemPingTable.
– interfaces — Added the ibmTcpipMvsIfTable and ibmTcpipMvsIfMcastTable.
– stack configuration — Added MIB objects corresponding to the IPCONFIG6 Profile statement parameters. Remote configuration of these parameters can be accomplished by snmp set operations on the MIB objects.
– routes — Added the ibmTcpipMvsRouteTable.
– TCP connections — Added the ibmTcpipMvsTcpConnectionTable.

- The following MIB objects in the IBM MVS TCP/IP Enterprise-specific MIB were deprecated:
  – ibmTcpipMvsLinkMcastTable - This table has been replaced by the new, version-neutral ibmTcpipMvsIfMcastTable.
  – The following OSA-Express MIB tables:
    - osaexpChannelTable
    - osaexpPerfTable
    - osaexpEthPortTable

  The OSA-Express Direct Subagent supports OSA-Express MIB data from the OSA-Express Direct Enterprise-specific MIB, which is similar to that in the above tables. The OSA-Express Direct Subagent has the added advantage of communicating directly with the OSA-Express adapters to retrieve the MIB data instead of requiring the OSA/SF facility. Refer to *zSeries OSA-Express Customer's Guide and Reference* for more information about the OSA-Express Direct Subagent and the OSA-Express Direct Enterprise-specific MIB.

Refer to the TCP/IP subagent section (in the Managing TCP/IP network resources with SNMP section) in *z/OS Communications Server: IP System Administrator's Commands* for a more detailed description of the supported MIB data.

Restrictions

None.

Dependencies

In order to retrieve SNMP IPv6 data, the TCP/IP stack associated with the subagent must be enabled for IPv6 support.

What this change affects

- Operations
- Customization

Using this function

If desired, you can perform the optional task in the following table.

Table 15. IPv6 support for SNMP TCP/IP subagent

Task	Procedure	Reference
Use the new or changed MIB objects from network management applications or from the z/OS UNIX snmp command.	The action to take depends on the management application. For the snmp command, no action is required. For the NetView SNMP command, use the most current copy of the sample MIBDESC.DATA file, which is shipped in SEZAINST(MIBDESC). Other management applications may require different changes.	TCP/IP subagent in *z/OS Communications Server: IP System Administrator's Commands*

Removal of SMIv1 version of SNMP IBM MVS TCP/IP Enterprise-specific MIB

- Support is removed for SMIv1 version of IBM MVS TCP/IP Enterprise-specific MIB module and it is no longer shipped.

  Until z/OS V1R6, two versions of the IBM MVS TCP/IP Enterprise-specific MIB module were shipped and installed in HFS directory /usr/lpp/tcpip/samples with the following file names:

  – mvstcpip.mib - the SMIv1 language version of the MIB module

  – mvstcpip.mi2 - the SMIv2 language version of the MIB module

  In z/OS V1R6 Communications Server, only the SMIv2 language version of the TCP/IP Enterprise-specific MIB module is shipped.

  The changes to the IBM MVS TCP/IP Enterprise-specific MIB module are also detailed in the REVISION section of this MIB module, which is installed in HFS directory /usr/lpp/tcpip/samples as file mvstcpip.mi2.

Restrictions

None.

What this change affects

- Customization

Using this function

No action is required other than to be aware that the support is removed for SMIv1 version and it is no longer shipped. If you want to continue using SMIv1, you can use publicly available tools to convert the SMIv2 MIB module (mvstcpip.mi2) to an SMIv1 MIB module.

TN3270E server address space option

The TN3270E server was changed to allow it to run in a separate address space from the TCP/IP stack address space. You may continue to run the TN3270E server as part of the TCP/IP address space.

You may want to consider running the TN3270E server separately from TCP/IP for the following reasons:

- The TN3270E server could run at a different priority than the stack.
- A second instance of the TN3270E server could be started.
- The TN3270E server could be stopped without stopping the stack. This makes it easier to reset the server or apply maintenance.

- Problem diagnosis is easier when the TN3270E server and stack are separate.

In addition, msys for Setup was updated to include support for starting a Telnet 3270 Server as a stand-alone application in its own address space.

Restrictions

The following restrictions apply:

- SNMP processing requires a one-to-one relationship with the Telnet server SNMP subagent and the TCP/IP SNMP agent. Therefore, even though multiple instances of Telnet can run, only one Telnet can be registered with one TCP/IP stack. Multiple Telnet instances require multiple TCP/IP stacks if SNMP data is being obtained from each stack. The subagent requires that Telnet have affinity to the stack where the agent resides when connecting to the agent. Use TCPIPJOBNAME to set up stack affinity.
- WLM requires that Telnet have affinity to a particular stack for successful registration.
- The SMF eight-character hostname field is filled in only if affinity has been specified. Also, the started task name will be the Telnet started task rather than the TCP/IP stack name.
- Telnet running in its own address space is not multilevel security compliant. For Telnet to be compliant, it must run as part of the TCP/IP stack.
- All Telnet commands must include the Telnet proc_name and not just a placeholder comma. Without the proc_name, the default is assumed to be a TCP/IP command.

Dependencies

UNIX System Services, VTAM, and TCP/IP must be active for Telnet to function properly.

What this change affects

- Availability
- Operations
- Diagnosis
- Storage

Using this function

If you want to use the TN3270E server address space option, perform the tasks in the following table.

Table 16. TN3270E server address space option

Task	Procedure	Reference
Set up a superuser with an OMVS segment.	Issue these commands: ADDUSER TN3270 ALTUSER TN3270 OMVS(UID(0) PROGRAM ('/bin/sh') HOME('/'))	UNIX System Services security considerations and Telnet in its own address space in *z/OS Communications Server: IP Configuration Guide*, *z/OS UNIX System Services Planning*, *z/OS Security Server RACF Security Administrator's Guide*, and *z/OS Security Server RACF Command Language Reference*

Table 16. TN3270E server address space option (continued)

Task	Procedure	Reference
Define the procedure in the RACF STARTED class and associate it to the user ID.	Issue these commands: RDEFINE STARTED TN3270*.* STDATA(USER(TN3270)) SETROPTS RACLIST(STARTED) REFRESH	Telnet in its own address space in *z/OS Communications Server: IP Configuration Guide*, *z/OS Security Server RACF Security Administrator's Guide*, and *z/OS Security Server RACF Command Language Reference*
Set up Telnet parameters in the profile dataset.	Specify the appropriate Telnet statements for the desired Telnet functions.	Accessing remote hosts using Telnet in *z/OS Communications Server: IP Configuration Guide*, TN3270 Telnet server in *z/OS Communications Server: IP Configuration Reference*, and *hlq*.SEZAINST(TNPROF)
Assign the profile dataset.	Specify the dataset name on the PROFILE DD card of the Telnet JCL.	*hlq*.SEZAINST(TNPROC)
If Telnet stack affinity is required, define stack affinity.	Specify the TCP/IP stack name on the TCPIPJOBNAME statement in TELNETGLOBALS.	Telnet in its own address space in *z/OS Communications Server: IP Configuration Guide* and TCPIPJOBNAME parameter in *z/OS Communications Server: IP Configuration Reference*
Start the procedure.	Issue the S TN3270 command.	*z/OS MVS System Commands*

Telnet SCS message table support

The TN3270 Telnet server will now support the SNA Character Stream (SCS) format for Unformatted System Services (USS) processes. The SCS format, which is supported by VTAM, will now also be supported by the Telnet server. If you are currently using SCS format tables in VTAM, you will be able to provide the same appearance to the end users. The SCS format is sent to the client as SSCP-LU data, which is supported by TN3270E clients only. TN3270 clients will continue receiving the 3270 format USS messages.

Restrictions

None.

What this change affects

- Customization
- Usability

Using this function

If you want to use the Telnet SCS message table support, perform the tasks in the following table.

Table 17. Telnet SCS message table support

Task	Procedure	Reference
Create an SCS format USS table.	Write, assemble, and linkedit a USS table.	Using the Telnet USS and INTERPRET support in *z/OS Communications Server: IP Configuration Guide* and Telnet USS table setup in *z/OS Communications Server: IP Configuration Reference*
Specify the table name on the USSTCP mapping statement.	Within the BEGINVTAM block, add the SCS USS table name to the mapping statement. For example, USSTCP EZBTPUST,EZBTPSCS *clid*.	USSTCP statement in *z/OS Communications Server: IP Configuration Reference*

FTP Callable API

A new CALL interface is provided for applications to invoke the FTP client programmatically. This API supports programs that utilize a standard call interface. Samples are provided for COBOL, PL/I, and Assembler.

Specifically, a new callable API to the z/OS CS FTP client supports a CALL instruction to the module EZAFTPKS. The CALL must pass parameters that include a place to put results of a request, the type of request, and other supporting parameters.

The supported requests are:
- INIT initializes the interface.
- SCMD sends an FTP subcommand.
- POLL checks status of an outstanding subcommand.
- GETL retrieves output related to a subcommand.
- TERM ends the interface.

The CALL interface is well-defined and is fully described in the following documents:
- FTP Callable Application Programming Interface (API) in *z/OS Communications Server: IP Programmer's Reference*
- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP User's Guide and Commands*

Restrictions

None.

Dependencies

Applications that invoke this new interface must have an OMVS segment defined (or defaulted).

What this change affects

- Application development

Using this function

If you want to use the CALL interface, perform the tasks in the following table. Refer to FTP Callable Application Programming Interface (API) in *z/OS Communications Server: IP Programmer's Reference* for more information.

Table 18. CALL interface

Task	Procedure
Use the FTP Callable Application Program Interface (API) in a user-written program to send requests to the z/OS FTP client.	Use the CALL instruction in a user-written program to invoke the API stub program EZAFTPKS.
Statically link the FTP Callable API stub program.	Add INCLUDE AEZAMODS(EZAFTPKS) to the link-edit job for the user-written program. EZAFTPKS is also shipped in SYS1.CSSLIB to enable dynamic load at execution. See "TCP/IP packaging process" on page 6 for information about distribution libraries.

FTP multi-byte character support

z/OS V1R6 Communications Server adds new support for double-byte character set data conversion for the z/OS FTP client and server.

Restrictions

The current double-byte character set (DBCS) support is provided by a set of client subcommands which are paired with a set of TYPE commands processed by the server as follows:

BIG5	TYPE B 8
EUCKANJI	TYPE B 2
JIS78KJ	TYPE B 4
JIS83KJ	TYPE B 3
KSC5601	TYPE B 6
SCHINESE	TYPE B 9
SJISKANJI	TYPE B 1
TCHINESE	TYPE B 7

The z/OS FTP client double-byte character set (DBCS) language support cannot be converted to the MBCS support if any of the following parameters is used on the listed subcommand:

SOSI ASCII	use ASCII shift-out x'1E' and shift-in x'1F'
SOSI EBCDIC	use EBCDIC shift-out x'0E' and shift-in x'0F'
SOSI SPACE	use space x'20' for both shift-out and shift-in
NOSO	pure DBCS - no shift-out or shift-in

The double-byte character set (DBCS) support at the z/OS FTP server cannot be converted to the multi-byte character support (MBCS) support if any of the following values highlighted in **bold** are used on the TYPE B command that is received by the server:

TYPE B x **S A**	indicates ASCII SOSI
TYPE B x **S E**	indicates EBCDIC SOSI
TYPE B x **S S**	indicates spaces for SOSI
TYPE B x **N**	indicates pure DBCS

Dependencies

The data type for data transfers using enhanced multi-byte character set must be ASCII, which is the default data type for an FTP session.

What this change affects

- Customization

Using this function

The FTP multi-byte character support is optional; the current method for DBCS support is not removed. If you decide you want to use the new MBCS method to achieve double-byte conversions, perform the tasks that are appropriate for you.

After you perform the appropriate tasks, eliminate loading DBCS conversion tables for languages migrated to MBCS support by deleting LOADDBCSTABLES statements in TCPIP.DATA for the languages that are migrated.

Refer to LOADDBCSTABLES in *z/OS Communications Server: IP Configuration Reference* for more information.

There are two task tables: Table 19 for users who connect from a z/OS FTP client to a non-z/OS server, and Table 20 on page 50 for users who connect from a non-z/OS client to a z/OS server.

Refer to FTP code page conversion in *z/OS Communications Server: IP Configuration Guide* and to FTP data conversion in *z/OS Communications Server: IP User's Guide and Commands* while you are completing the tasks.

Table 19. FTP multi-byte character support for users who connect from a z/OS FTP client to a non-z/OS server

Task	Procedure
Request data conversion for IBM BIG5 DBCS to replace BIG5 (NOTYPE.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MB=(IBM-937,IBM-950) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-937,IBM-950)
Request data conversion for Japanese EUC to replace EUCKANJI (NOTYPE.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MB=(IBM-930,IBM-eucJP) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-930,IBM-eucJP)
Request data conversion for JIS 1978 kanji with Jisroman shift-in escape sequence to replace JIS78KJ (NOTYPE J.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MB=(IBM-930,IBM-5053) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-930,IBM-5053)
Request data conversion for JIS 1978 kanji with ASCII shift-in escape sequence to replace JIS78KJ (NOTYPE or JIS78KJ (NOTYPE A.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MB=(IBM-939,IBM-5055) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-939,IBM-5055)

Table 19. FTP multi-byte character support for users who connect from a z/OS FTP client to a non-z/OS server (continued)

Task	Procedure
Request data conversion for JIS 1983 kanji with Jisroman shift-in escape sequence to replace JIS83KJ (NOTYPE J.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MB=(IBM-930,IBM-5052) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-930,IBM-5052)
Request data conversion for JIS 1983 kanji with ASCII shift-in escape sequence to replace JIS83KJ (NOTYPE or JIS83KJ (NOTYPE A.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MB=(IBM-939,IBM-5054) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-939,IBM-5054)
Request data conversion for Korean Standard Code to replace KSC5601 (NOTYPE.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MBD=(IBM-933,IBM-949) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-933,IBM-949)
Request data conversion for Simplified Chinese to replace SCHINESE (NOTYPE.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MBD=(IBM-935,IBM-1381) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-935,IBM-1381)
Request data conversion for Shift JIS kanji SJISKANJI (NOTYPE.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MBD=(IBM-930,IBM-932) Or code in FTP.DATA for the client: ENCODING MBCS MBDATACONN (IBM-930,IBM-932)
Request data conversion for Traditional Chinese to replace TCHINESE (NOTYPE.	Enter at the FTP client: LOCSITE ENCODING=MBCS LOCSITE MBD=(IBM-937,IBM-948) Or code in FTP.DATA for the client: ENCODING MBCS MDATACONN (IBM-937,IBM-948)

Table 20. FTP multi-byte character support for users who connect from a non-z/OS client to a z/OS server

Task	Procedure
Request data conversion for IBM BIG5 DBCS to replace TYPE B 8.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MB=(IBM-937,IBM-950) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-937,IBM-950)
Request data conversion for Japanese EUC to replace TYPE B 2.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MB=(IBM-930,IBM-eucJP) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-930,IBM-eucJP)
Request data conversion for JIS 1978 kanji with Jisroman shift-in escape sequence to replace TYPE B 4 R.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MB=(IBM-930,IBM-5053) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-930,IBM-5053)
Request data conversion for JIS 1978 kanji with ASCII shift-in escape sequence to replace TYPE B 4 A.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MB=(IBM-939,IBM-5055) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-939,IBM-5055)
Request data conversion for JIS 1983 kanji with Jisroman shift-in escape sequence to replace TYPE B 3 R.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MB=(IBM-930,IBM-5052) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-930,IBM-5052)
Request data conversion for JIS 1983 kanji with ASCII shift-in escape sequence to replace TYPE B 3 A.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MB=(IBM-939,IBM-5054) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-939,IBM-5054)

Table 20. FTP multi-byte character support for users who connect from a non-z/OS client to a z/OS server (continued)

Task	Procedure
Request data conversion for Korean Standard Code to replace TYPE B 6.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MBD=(IBM-933,IBM-949) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-933,IBM-949)
Request data conversion for Simplified Chinese to replace TYPE B 9.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MBD=(IBM-935,IBM-1381) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-935,IBM-1381)
Request data conversion for Shift JIS kanji to replace TYPE B 1.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MBD=(IBM-930,IBM-932) Or code in FTP.DATA for the server: ENCODING MBCS MBDATACONN (IBM-930,IBM-932)
Request data conversion for Traditional Chinese to replace TYPE B 7.	Enter at the FTP client: QUOTE SITE ENCODING=MBCS QUOTE SITE MBD=(IBM-937,IBM-948) Or code in FTP.DATA for the server: ENCODING MBCS MDATACONN (IBM-937,IBM-948)

Netstat enhancements

The documentation of the Netstat command in *z/OS Communications Server: IP System Administrator's Commands* has been completely restructured to improve the format and provide more comprehensive descriptions for the various Netstat reports.

z/OS V1R6 Communications Server introduces the following changes to the existing Netstat reports:

- The z/OS UNIX netstat/onetstat command heading is changed to use the generic 'NETSTAT' instead of 'onetstat' so that the command can generate the same reports from either the TSO or the z/OS UNIX shell environment.
- The Netstat ARP/-R report is changed to display the following information:
  - The NSAP instead of ATMNSAP for ATM link types
  - The link type for HiperSockets links.
- The Netstat DEVLINKS/-d report is changed to display the following information:

- A value of n/a instead of 0 in the NetNum field for interfaces and links other than CTC and LCS because the NetNum field is not applicable to them.
- A value of n/a instead of 0 in the QueSize field for interfaces other than IPAQENET6 and links other than ATM and LCS because the QueSize field is not applicable to them.
- A value of MPCPTP instead of MPC in the DevType for MPCPTP devices.
- A value of MPCPTP instead of MPC in the LnkType field for MPCPTP links.
- A value of MPCPTP6 instead of MPC6 in the IntfType field for MPCPTP6 interfaces.
- A value of Packed/None instead of Yes/No in the CfgPacking fields for CLAW devices.
- A value of Packed/None instead of Packed/Unpacked in the ActPacking fields for CLAW devices.

• The Netstat CONFIG/-f report is changed to display the following information:
- Some of values from 01/00 to Yes/No.
- The field name from NOUdpQueueLimit to UdpQueueLimit.

• Changed the Netstat ROUTE/-r report to display the following information:
- The DELAYACKS/NODELAYACKS setting information when the DETAIL modifier is specified.
- The MTU size for IPv4 routes in both LONG and SHORT formats of the report when the DETAIL modifier is specified.
- The field name MTU instead of Pktsize for IPv6 routes.
- The prefix length information for IPv4 routes in the SHORT format to show the subnet mask information.

• The existing port number filter (PORT/-P) support is added to PORTLIST/-O report.

Refer to Netstat in *z/OS Communications Server: IP System Administrator's Commands* for more information about the Netstat command and options.

Restrictions

None.

What this change affects

- Diagnosis
- Usability

Using this function

If you want to use the Netstat enhancements, perform the task in the following table. Refer to Netstat in *z/OS Communications Server: IP System Administrator's Commands* for more information.

Table 21. Netstat enhancements

Task	Procedure
View TCP/IP information by using the Netstat command.	Specify the Netstat command with the proper options.

Job specific source IP addressing

Job specific source IP addressing establishes an IP address to be used as the source IP address for TCP connections initiated by an application which has not bound the socket or has bound the socket to inaddr_any or inaddr6_any before issuing the connect().

In addition, job specific source IP addressing allows a specific job or set of jobs to have a unique source IP address for outbound initiated connections, different from other jobs, and independent of the order of addresses in the HOME list. If it is a VIPA source IP address designation, it overrides TCPSTACKSOURCEVIPA and normal SOURCEVIPA processing. This function would be useful when a job communicates with specific partners, by ensuring that a single address gets used as the source address, which can simplify firewall configuration. It may also be useful for a server application supported by Sysplex Distributor, so the Distributed DVIPA can be used as the source IP address for connections initiated by the server application instances.

If NETACCESS INBOUND is active on this stack and the job specific source IP address is configured into a network security zone, the user ID associated with the job must have READ permission to the EZB.NETACCESS profile for that network security zone.

Restrictions

This function applies only to outbound TCP connection requests. It does not apply to UDP datagrams or raw socket outbound data.

Incompatibilities

An application matching on a PORT statement with the BIND parameter will supersede the job specific source IP address selection.

Dependencies

If the same job specific VIPA source IP address is used on more than one z/OS TCP/IP stack, then the job specific source VIPA IP address should be a Distributed DVIPA with SYSPLEXPORTS enabled.

What this change affects

- Availability
- Installation
- Operations
- Usability
- Customization

Using this function

If you want to use the job specific source IP addressing, perform the tasks in the following table.

Table 22. Job specific source IP addressing

Task	Procedure	Reference
Designate that a specific job or jobs should use a particular Virtual IP Address or interface name (static VIPA or Dynamic VIPA, or real IP address) as the source address for outbound TCP connections.	Use the SRCIP/ENDSRCIP profile statement to designate the IP address or the interface name to be used by that job or jobs.	SRCIP statement in *z/OS Communications Server: IP Configuration Reference*
Display information about current job specific source IP address designations active on a TCP/IP stack.	Use the Netstat SRCIP/-J command to display the current job specific source IP address designations active on a z/OS TCP/IP stack.	Netstat in *z/OS Communications Server: IP System Administrator's Commands*
Change or remove a job specific source IP address designation.	Change or remove the JOBNAME entries from the previously defined SRCIP/ENDSRCIP profile statement, then issue the VARY TCPIP,,OBEYFILE command for the modified SRCIP/ENDSRCIP profile statement. The new designations will completely replace the existing designations.	SRCIP statement in *z/OS Communications Server: IP Configuration Reference*

Socket option access control

Support is added to control the ability of a z/OS application to set the SO_BROADCAST socket option required to send broadcast datagrams. Without this support, the ability to send UDP or RAW datagrams to a broadcast address could be abused to create packet flood attacks or to circumvent network access controls.

Socket option access control is provided with the SERVAUTH class resource profile EZB.SOCKOPT.sysname.tcpname.SO_BROADCAST. If this profile is defined, users of applications that set the SO_BROADCAST socket option must be permitted at least READ authority to this profile. Certain TCP/IP applications attempt to send datagrams to a broadcast address.

See Socket option access control in *z/OS Communications Server: IP Configuration Guide* for a list of TCP/IP programs that would require users to have permission to this new profile.

Restrictions

None.

What this change affects

- Security

Using this function

If you want to use the socket option access control enhancement, perform the tasks in the following table. Refer to TCP/IP resource protection and Socket option access control in *z/OS Communications Server: IP Configuration Guide* and *z/OS Security Server RACF Command Language Reference* for more information.

Table 23. Socket option access control enhancement

Task	Procedure
Activate the SERVAUTH class.	Issue the following commands: SETROPTS CLASSACT(SERVAUTH) SETROPTS RACLIST(SERVAUTH)
Define the Socket Option Resource Profile.	Issue the following commands: RDEFINE SERVAUTH EZB.SOCKOPT.*.*.SO_BROADCAST. UACC(NONE) SECLABEL(SYSLOW)
Permit certain users or programs.	Issue the following commands: PERMIT EZB.SOCKOPT.*.*.SO_BROADCAST CL(SERVAUTH) ACCESS(READ) ID(OMPROUT) PERMIT EZB.SOCKOPT.*.*.SO_BROADCAST CL(SERVAUTH) ACCESS(READ) ID(*) WHEN(PROGRAM(ORPCINFO))
Make the changes available.	Issue the following command: SETROPTS RACLIST(SERVAUTH) REFRESH

Trivial FTP Daemon (TFTPD) specific bind

Trivial FTP Daemon (TFTPD) has been changed from a generic server (that binds to in6addr_any or inaddr_any) to allow it to optionally bind specifically to an IP address using the new -b start option. This provides the flexibility to run multiple copies of TFTPD on the same stack. In a multilevel secure environment, this allows servers to be run with different security labels.

Restrictions

None.

What this change affects

- Availability
- Usability
- Security

Using this function

If you want to use the Trivial FTP Daemon (TFTPD) specific bind enhancement, perform the tasks in the following table.

Table 24. Trivial FTP Daemon (TFTPD) specific bind enhancement

Task	Procedure	Reference
Configure multiple TFTPD servers on a single stack.	Start multiple TFTPD jobs with each job specifying a unique IP address for the -b start option.	*z/OS Communications Server: IP Configuration Guide* and Starting TFTPD as a procedure in *z/OS Communications Server: IP Configuration Reference*

Table 24. Trivial FTP Daemon (TFTPD) specific bind enhancement (continued)

Task	Procedure	Reference
When running in a multilevel secure environment, configure a TFTPD server for each security zone/label.	Start each TFTPD job with a different user ID and default security label.	*z/OS Communications Server: IP Configuration Guide* and Starting TFTPD as a procedure in *z/OS Communications Server: IP Configuration Reference*

Multilevel security enhancements

Multilevel security is enhanced in the following areas:

- "Multilevel security configuration consistency check"
- "Simple Network Time Protocol Daemon (SNTPD)" on page 57
- "Sendmail" on page 58

If you are planning to run in a multilevel secure environment, see Preparing for TCP/IP networking in a multilevel secure environment in *z/OS Communications Server: IP Configuration Guide*.

Multilevel security configuration consistency check

Secure communication in a multilevel secure environment requires configuration of several statements in the PROFILE.TCPIP and security server resource profiles in the SERVAUTH, SECLABEL and STARTED classes. Inconsistencies in this configuration can allow unintended communication or prevent intended communication.

When the RACF MLACTIVE option is set, TCP/IP checks the current stack profile settings and the resource profiles for consistency. Consistency checking occurs at TCP/IP initialization, when a VARY,TCPIP,,OBEYFILE command is processed and when a RACLIST REFRESH is done on the SERVAUTH or SECLABEL class.

TCP/IP writes an informational message to the job log for each inconsistency detected. If inconsistencies are found, a final message, EZD1217I, summarizing the number of problems found is written to the system console. You should check the job log for messages in the range EZD1219I-EZD1234I whenever message EZD1217I appears on the system console. You should correct your configuration as indicated by the job log messages until TCP/IP no longer detects any errors.

TCP/IP's default behavior is to continue running when inconsistent security configurations are detected. If you plan to run in a multilevel secure environment, it is recommended that you specify GLOBALCONFIG MLSCHKTERMINATE in your PROFILE.TCPIP when running production workloads and GLOBALCONFIG NOMLSCHKTERMINATE while you are making planned changes to your security environment.

As a result of the multilevel security configuration consistency check, Netstat is changed and it may affect automation. Refer to *z/OS Migration* for migration actions.

Restrictions

None.

Dependencies

The RACF MLACTIVE option must be active to enable consistency checking. The GLOBALCONFIG [NO]MLSCHKTERMINATE option in PROFILE.TCPIP is ignored when NOMLACTIVE is set.

What this change affects

- Diagnosis
- Usability
- Security

Using this function

If you want to use this enhancement, perform the tasks in the following table. Refer to Changing your multilevel secure networking environment in *z/OS Communications Server: IP Configuration Guide* and *z/OS Security Server RACF Command Language Reference* for more information.

Table 25. Multilevel security configuration consistency check

Task	Procedure
Provide a controlled environment for security configuration changes.	Drain the system of all production work by issuing the following command: SETROPTS MLACTIVE MLSTABLE MLQUIET
Disable stack termination on consistency check failures.	Issue the following command: GLOBALCONFIG NOMLSCHKTERMINATE
Make changes to security configuration until no consistency check errors are reported.	Do the following: 1. Edit the PROFILE.TCPIP or use the VARY TCPIP,,OBEYFILE command. 2. Modify the security server profiles by using the following RACF commands: RDEFINE, RALTER resource profiles SETROPTS RACLIST(SERVAUTH SECLABEL STARTED) REFRESH
Enable stack termination on consistency check failures.	Issue the following command: GLOBALCONFIG MLSCHKTERMINATE
Return to a production environment.	Issue the following command: SETROPTS MLACTIVE MLSTABLE NOMLQUIET Restart production work.

Simple Network Time Protocol Daemon (SNTPD)

If TIMED is deployed in your multilevel secure environment or if you have a need to synchronize clients and servers in your multilevel secure network, Simple Network Time Protocol Daemon (SNTPD) is the preferred, or strategic, time daemon. It is now supported in the multilevel secure environment.

The TIMED protocol allows for a precision of one second; (S)NTP allows for a more precise time adjustment. In addition, SNTPD has a number of useful functions that allow clients and servers to estimate the network delay between each other. A client can adjust the timestamp it receives from an (S)NTP server to account for network delay.

Restrictions

None.

What this change affects

- Availability
- Usability
- Security

Using this function

If you want to use the SNTPD enhancement, perform the task in the following table. Refer to Planning for applications in a multilevel secure environment in *z/OS Communications Server: IP Configuration Guide* and SNTP daemon in *z/OS Communications Server: IP Configuration Reference* for more information.

Table 26. SNTPD enhancement

Task	Procedure
Configure SNTPD in a multilevel secure environment.	Start SNTPD from a user whose security label is SYSMULTI.

Sendmail

z/OS UNIX Sendmail can now run in a multilevel security environment.

Restrictions

Multiple copies of the Sendmail server must be run with different security labels.

Incompatibilities

The Sendmail server will not be secure if it is run under a user ID with a SYSMULTI security label.

What this change affects

- Availability
- Usability
- Security

Using this function

If you want to use the Sendmail enhancement, perform the tasks in the following table.

Table 27. Sendmail enhancement

Task	Procedure	Reference
Run the Sendmail daemon in a multilevel secure environment.	Update the Sendmail daemon configuration to run a Sendmail daemon for each security zone/label.	Planning for applications in a multilevel secure environment in *z/OS Communications Server: IP Configuration Guide , sendmail by O'Reilly & Associates, Inc. (ISBN 1-56592-839-3)* and *z/OS Security Server RACF Security Administrator's Guide*
Run the Sendmail client or Mail Submission Program (MSP) in a multilevel secure environment.	Update the Sendmail configuration to run a Sendmail client or MSP for each security zone/label.	Planning for applications in a multilevel secure environment in *z/OS Communications Server: IP Configuration Guide* and *sendmail by O'Reilly & Associates, Inc. (ISBN 1-56592-839-3)*

Support 64-bit virtual addresses for X Windows and Motif

z/OS V1R6 Communications Server provides new versions for the X Window System and Motif libraries. The new libraries are based upon X Window System X11R6.6 and Motif 2.1.30. Details on the functions available with the new versions are provided in X Window System Interface in the z/OS Communications Server in *z/OS Communications Server: IP Programmer's Reference*.

In addition to the new functions available with the newer versions, these libraries are provided with the following characteristics:

- Static Archive Libraries for 31-bit mode and 64-bit mode compiled with XPLINK and FLOAT(IEEE)
- Dynamic Libraries (DLLs) for 31-bit mode and 64-bit mode compiled with XPLINK and FOAT(IEEE)

While applications using the new libraries are not required to be compiled with FLOAT(IEEE), there are performance advantages to doing so.

The old X Windows and Motif libraries (X116.1 and Motif 1.2) are still provided and are compatible with existing programs. They are compiled with 31-bit non-XPLINK and use IBM Hexadecimal Floating Point. These DLLs do not contain new function; therefore, if you continue to compile with these old libraries, some changes are necessary to use the correct headers.

Details for compiling and linking your application with the old and the new libraries are provided in Compiling and linking OSF/Motif and X Window System applications in *z/OS Communications Server: IP Programmer's Reference*.

Restrictions

To use the new libraries, your application must be compiled and linked with the following characteristics:

- The XPLINK option must be used on the compile and link steps.
- DLL must be used on the compile and link steps, even if you plan to use static linking.
- If you are using dynamic linking, you must link your application with the correct side-deck for the addressing mode in which you are compiling.

  For example, if you compile in 31-bit mode (the default), you must link with the X11_31.x side deck. If you compile in 64-bit mode, then you must link your application with the X11_64.x side deck. At run time, the appropriate DLL will be located by using the value of the LIBPATH environment variable.

Native ASCII is not supported for X11 or Motif applications.

Incompatibilities

The C++ class wrapper programming interface to Motif is no longer supported by the new Motif libraries. If you require this function, then you must continue to use the Motif 1.2 libraries or change your application.

Dependencies

All applications that will use the new function must be compiled and linked with the XPLINK option. To run 64-bit applications, you must be running on a machine that supports 64-bit applications and you must compile and bind with the LP64 option.

What this change affects

- Application development
- Usability
- Installation

Using this function

If you want to use the support for 64-bit Virtual Addresses for X Windows and Motif, perform the desired tasks in the following table. Refer to X Window System Interface in the z/OS Communications Server in *z/OS Communications Server: IP Programmer's Reference* for more information.

Table 28. Support 64-bit Virtual Addresses for X Windows and Motif

Task	Procedure
Run existing 31-bit X Window or Motif applications.	If your application is sensitive to the locale, then you need to export the XLOCALEDIR environment variable to point to the locale data files for X11R6.1. This is necessary because the format of the data files has changed with X11R6.6 and X11R6.6 is the default. For example, export XLOCALEDIR="/usr/lpp/tcpip/X11R6/lib/X11/locale. For dynamically linked applications, the DLL names have not changed. Programs linked with the static libraries from previous releases will continue to operate on this release.
Recompile existing 31-bit X Window applications to use the old libraries (X11 6.1 and Motif 1.2) and the old header files for these releases.	Change your makefile or JCL to use the -I option and specify the HFS directory that contains the old header files (/usr/lpp/tcpip/X11R6/include). If you do not do this, your application will pick up the new header files by default and may not compile or operate correctly. For dynamic linkage, the DLL and side deck names have not changed. For static linkage, the library names have not changed. However, the symbolic links from /usr/lib now point to the new libraries. To use the old libraries, use the -L option on the link step to tell the binder where to find the X and Motif libraries. For example, -L/usr/lpp/tcpip/X11R6/lib.
Use the new 31-bit X Window applications and libraries.	If you have an existing C X Window System or Motif application that is to be recompiled to use the new 31-bit libraries, be aware of the following and take any necessary action: 1. The application's C parts must be compiled with the XPLINK and DLL options. 2. The header files from /usr/include should be used. This is the default. 3. Link the code with the XPLINK and DLL linker options. For dynamic linking, you must link with the side decks that use the _31 suffix. For example, X11_31.x. For static linking, the library names have not changed and are still symbolically linked from /usr/lib/. 4. At runtime, dynamically linked applications must have /usr/lib in the LIBPATH environment variable.
Use the new 64-bit X Window applications and libraries.	If you have an existing C X Window System application that is to be converted, do the following: 1. Visually inspect the source code and make changes that are required for 64-bit compatibility. The compiler option, WARN64, can be used to help find 64-bit compatibility problems with existing code. 2. Compile the code in 64-bit mode using the LP64 and XPLINK compile options. 3. Link the code with the LP64 and XPLINK linker options. For dynamic linking, you must link with the side decks that use the _64 suffix, such as X11_64.x. For static linking, the library names have not changed and are still symbolically linked from /usr/lib/. 4. At runtime, ensure that dynamically linked applications have /usr/lib in the LIBPATH environment variable.

SYNAD exit for SMTP

In some cases, the SMTP server can experience an ABENDS001 when processing JES spool files. A new, optional configuration statement, DELETEBADSPOOLFILE has been added to the SMTPPROC configuration data set. When specified, the SMTP server will delete the bad spool file and continue to run.

Restrictions

None.

What this change affects

- Availability

Using this function

If you want to use SYNAD exit for SMTP, perform the desired tasks in the following table.

Table 29. SYNAD exit for SMTP

Task	Procedure	Reference
Enable optional statement to change SMTP's default behavior.	Code in the SMTP configuration file the statement DELETEBADSPOOLFILE.	Configuration process (under the heading Checklist for working within the SMTP environment) in *z/OS Communications Server: IP Configuration Guide* and DELETEBADSPOOLFILE statement in *z/OS Communications Server: IP Configuration Reference*
New errors messages may be displayed on the system console due to this new function.	Follow the instructions within error messages.	*z/OS Communications Server: IP Messages Volume 1 (EZA)*

SYSTCPDA packet trace formatting

In z/OS V1R6 Communications Server, the CTRACE SYSTCPDA packet trace formatting extends to:

- Formatting of RIPng Packets for IPv6 (new for z/OS V1R5 Communications Server)
- Formatting of OSPF Version 3 packets for IPv6
- Formatting of Enterprise Extender packets
- Formatting of LPR packets
- Formatting of POP3 packets
- Formatting of SYSLOG packets

In addition, the following enhancements are made in z/OS V1R6 Communications Server:

- The formatting of TELNET packets is enhanced to format the 3270 data streams.
- The SNIFFER options are extended to include the TCPDUMP data output format.
- The device type of IPAQIDIO6 is added to the list of device type filters.

- A new filter is provided: CID(x'hhhh') for data trace records. The CID is the same value from the NETSTAT CONN display.
- A new filter is provided: FLAG(DATA). This keyword selects packets that contain more than IP headers and protocol headers.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

If you want to use the new SYSTCPDA formatting filter enhancements, perform the tasks in the following table. Refer to Packet trace (SYSTCPDA) for TCP/IP stacks in *z/OS Communications Server: IP Diagnosis Guide* for details.

Table 30. SYSTCPDA packet trace formatting

Task	Procedure
Format RIPng packets.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((RIPNG)).
Format OSPF Version 3 packets.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((OSPF)).
Format Enterprise Extender packets.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((EE)).
Format LPR packets.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((PORT(515))).
Format POP3 packets.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((PORT(110))).
Format SYSLOG packets.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((PORT(514))).
Format TELNET 3270 screens.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((TELNET(SUMMARY))).
Format TELNET 3270 data stream.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((TELNET(DETAIL))).
Create TCPDUMP output SNIFFER data file.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((SNIFFER(TCPDUMP))).
Select packets transferred over QDIO for IPv6.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((DEVTYPE(IPAQIDIO6))).
Select packets with protocol data.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((FLAG(DATA))).
Select data trace records for a specific CID.	Specify CTRACE COMP(SYSTCPDA) OPTIONS((CID(nnnn))).

Chapter 4. V1R5 IP new function summary

This chapter includes a section for every function or enhancement introduced for IP in z/OS V1R5 Communications Server. The sections include the following 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. The tables include references to the documents that contain more detailed information for each task.

See Table 8 on page 25 for a complete list of the functional enhancements of the current and recent releases.

Refer to *z/OS Migration* for information about how to maintain the functional behavior of previous releases. Refer to *z/OS Summary of Message and Interface Changes* for information on new and changed messages and interfaces.

General considerations

In addition to the function-specific tasks of this chapter, be aware of the following general considerations:

- FFST™ module EPWSTUB must be included in Fixed LPA. This is also true for previous releases. This can be accomplished by specifying this in a SYS1.PARMLIB(IEAFIXxx) member. For example:

  ```
  INCLUDE LIBRARY(FFST.SEPWMOD2) MODULES(EPWSTUB)
  ```

  Where FFST.SEPWMOD2 is the library in which EPWSTUB resides.
- The PASCAL Application Programming Interface (API) MonQuery function has a return code value of UNAUTHORIZEDuser as a possible return code in certain error scenarios. The UNAUTHORIZED user return code value existed previously in some applications but it is new in z/OS V1R5 Communications Server for Simple Mail Transfer Protocol (SMTP).
- Keywords and their abbreviations should not be used for any user defined name because it gives unpredictable results. For example, do not use the abbreviation PORTS for SMFCONFIG PORTSTATISTICS in the PROFILE.TCPIP.
- When using a GetHostId/GetHostName vnode operation (a call made to the stack PFS by the USS LFS when an application issues the gethostid() or gethostname() function), be aware that starting in z/OS V1R5 Communications Server, the stack will verify the caller has authorization to the EZB.STACKACCESS.*mvsname.tcpname* (where *mvsname* is the MVS system name and *tcpname* is the TCP job name resource) in the SERVAUTH class. This will prevent applications in a C_INET environment from receiving the host name or default IP address of a stack that they are not then permitted to use. If the resource profile exists and the user does not have READ authority, they will receive a return and reason code of EACCES and JRNOTAUTHSTACK. The user should set affinity to the stack he is permitted to use before re-running the application.

Refer to the chapter on security in *z/OS Communications Server: IP Configuration Guide* for more information.

- If, in previous releases, you were using Enterprise Extender and automating on the message EZZ4313I to activate VTAM definitions, be aware that you can no longer do this in z/OS V1R5 Communications Server. In previous releases, TCP/IP issued message EZZ4313I for MPCPTP devices before the LINK became active. In z/OS V1R5 Communications Server, TCP/IP does not issue message EZZ4313I until the LINK is marked active.
- A set of new sample programs illustrates IPv6:
  - EZACIC6C - IPv6 child server program written in the COBOL language
  - EZACIC6S - IPv6 iterative server program also written in the COBOL language
  - EZACICAC - Child server program written in the assembler language
  - EZACICAS - Iterative server program written in the assembler language
- FTP issues message EZYFT47I for every statement coded in FTP.DATA that it ignores. A new configuration statement, SUPPRESSIGNOREWARNINGS, can be coded in either the FTP client's or FTP server's FTP.DATA to suppress message EZYFT47I.

Full Virtual LAN support for OSA-Express

z/OS V1R5 Communications Server extends Virtual LAN (VLAN) support by allowing you to assign a Virtual LAN identifier (VLAN ID) to an OSA-Express link or interface. This allows all packets using an OSA-Express to carry a VLAN ID, and thus segregate traffic into different VLANs without needing multiple real LANs or creating new subnetworks.

Restrictions

The following restrictions apply:

- For a given OSA-Express, a stack can only specify one VLAN ID for IPv4 traffic and one VLAN ID for IPv6 traffic. The IPv4 VLAN ID may be different from the IPv6 VLAN ID. Note that when multiple stacks share an OSA-Express, each stack sharing the OSA may specify a different VLAN ID.
- The VLANID parameter of the DEVICE, LINK, and INTERFACE statements interacts with the PRIRouter and SECRouter parameters. If you configure both a VLANID and either PRIRouther or SECRouter, then this TCP/IP instance will act as a router for this VLAN ID only. Datagrams that are received at this device for an unknown IP address will only be routed to this TCP/IP instance if it is VLAN tagged with this VLAN ID. For additional information regarding how VLANID interacts with PRIRouting, refer to *z/OS Communications Server: IP Configuration Reference*.

Dependencies

This function is only available for an OSA-Express configured in QDIO mode. You must be running on IBM @server zSeries 990 or IBM @server zSeries 900 at system driver level 3G to use this function. It requires z/OS V1R5, an OSA-Express Ethernet feature, and OSA microcode 3.33.

Incompatibilities

When you assign a VLAN ID to the OSA-Express interface to help manage where traffic can go, all the packets that flow through the OSA-Express interface have that VLAN identifier associated with them. This means that for the OSA-Express interface, that assigned VLAN ID is included in your packet. If a switch or router

that does not support VLAN ID is encountered, the switch may not know what to do with your packet; therefore, there is no guarantee that your packet will make it past that switch (unpredictable results may occur). To avoid this situation, design your network paths to ensure that you have a clear VLAN path from all points if you are using Virtual LANs.

What this change affects

- Customization
- Performance

  This enhancement may improve performance because as media types grow in bandwidth, users of LANs must increasingly handle larger amounts of data traffic for some IP addresses of which the users have no interest. Virtual LANs enable traffic to be segregated in such a way that the users do not see this traffic.

Using this function

If you want to use the full Virtual LAN support **for IPv4 traffic**, perform the task in the following table. If you want to use the full Virtual LAN support **for IPv6 traffic**, see "IPv6 support — Full Virtual LAN (VLAN) support for OSA-Express" on page 92.

Table 31. Full Virtual LAN support for IPv4 traffic

Task	Procedure	Reference
Specify the Virtual LAN identifier desired **for IPv4 traffic** through an OSA-Express interface.	Define the VLANID keyword on the LINK statement for the MPCIPA device statement representing this OSA-Express.	*z/OS Communications Server: IP Configuration Reference*

Enterprise Extender enhancements

In z/OS V1R5 Communications Server, the support for Enterprise Extender is enhanced in two areas:

- Enterprise Extender, IBM's strategic mechanism for integrating SNA and IP networks, is IPv6-enabled.
- You can specify a hostname, instead of an IP address, for use by remote Enterprise Extender endpoints wishing to connect to an Enterprise Extender node. The remote endpoint will perform name-to-address resolution on the hostname to obtain the correct IP address for Enterprise Extender connection establishment, reducing some of the costs previously associated with Enterprise Extender in a multiple enterprise environment. The ability to exchange hostnames, instead of explicit IP addresses, allows Enterprise Extender nodes to exploit the use of network address translation (NAT) between Enterprise Extender connection endpoints much more easily than in previous releases.

Refer to "Enterprise Extender enhancements" on page 205 for details of these enhancements, including restrictions, incompatibilities, and exploitation information.

Sysplex enhancements

In z/OS V1R5 Communications Server, sysplex is enhanced in the following areas:

Sysplex Distributor round-robin distribution

Sysplex Distributor uses Workload Manager (WLM) information to distribute incoming work according to varying LPAR capacities, sending more work where there is more capacity. For some applications though, distributing according to WLM capacity and policy recommendations is not appropriate, such as when connections are to be spread evenly among server instances.

z/OS V1R5 Communications Server introduces a new DISTMETHOD ROUNDROBIN parameter on the VIPADISTRIBUTE statement that may be used to assign incoming connections for the Distributed DVIPA among available server instances in a round-robin method.

Notes:

1. Although Sysplex Distributor round-robin distribution was introduced in V1R5, it is available for z/OS V1R4 Communications Server with APAR PQ76866.
2. The DISTMETHOD option does not have any effect on incoming connection requests that have an active affinity established to a specific server instance (by way of the TIMEDAFFINITY parameter). When an affinity exists, it has priority over the DISTMETHOD setting.

What this change affects

- Availability
- Operations
- Customization
- Usability

Restrictions

The following restrictions apply:

- If a VIPADISTRIBUTE statement is specified on a backup routing stack, and the VIPADISTRIBUTE statement on the primary routing stack contains the DISTMethod ROUNDROBIN parameter value, the VIPADISTRIBUTE statement must also have the DISTMETHOD ROUNDROBIN to continue round-robin distributions.
- If a VIPADISTRIBUTE statement is changed (from DISTMETHOD ROUNDROBIN to DISTMETHOD BASEWLM, or from DISTMETHOD BASEWLM to DISTMETHOD ROUNDROBIN) by using the VARY TCPIP,,OBEYFILE command, when the Distributed DVIPA already has active connections to target server instances, only the distribution of future connection requests will be affected. Existing connections will be unaffected by this change.

Co-existence considerations

The routing stack and all backup routing stacks for a Distributed DVIPA should be at z/OS V1R4 with the enabling PTF or later for this function to work properly in scenarios of takeover.

Using this function

If you want to use Sysplex Distributor round-robin distribution, perform the desired tasks in the following table.

Table 32. Sysplex Distributor round-robin distribution

Task	Procedure	Reference
Enable round-robin distribution of incoming connection requests for a Distributed DVIPA, regardless of the setting of IPCONFIG SYSPLEXROUTING and WLM or policy information.	Specify the DISTMETHOD ROUNDROBIN parameter on the VIPADISTRIBUTE statement.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Display round-robin distribution setting.	Use Netstat VIPADCFG/-F and VDPT/-O to display distribution method setting.	*z/OS Communications Server: IP System Administrator's Commands*
Remove round-robin distribution setting.	Specify the DISTMETHOD BASEWLM parameter on the VIPADISTRIBUTE statement.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Workload distribution (Application Server Affinity) enhancements

The Timed Affinity feature of Sysplex Distributor allows affinities to be established between a specific client (identified by its IP address) and a particular instance of a server application for which work is being balanced with Sysplex Distributor, using a Distributed Dynamic VIPA. This feature ensures that a client that establishes a relationship with a server will be directed to that particular server for subsequent connections.

Two examples show how this enhancement is a benefit:

- TN3270 users who need to establish printer sessions through TN3270 may now have their workload distributed with Sysplex Distributor.
- Complex Web applications requiring multiple connections from the browser may now have workload distributed to Hypertext Transfer Protocol (HTTP) servers using Sysplex Distributor.

Restrictions

The following restrictions apply:

- The longest affinity that may be established after the last connection from the client is closed is 9999 seconds, or about 2.8 hours.
- Timed Affinity depends on the source IP address of a connection request to distinguish one client from another. If many real clients are sharing the same IP address, as could be the case with proxy connectivity, or firewall Network Address Translation, or many clients on z/OS or OS/390 using SOURCEVIPA, or multiple hosts in a z/OS sysplex using the same TCPSTACKSOURCEVIPA address, then client connections which could have been balanced will be routed to the same server instance.

- Affinity information needs to be handled on the Sysplex Distributor routing stack, backup stacks, and target stacks. If a target stack is not z/OS V1R5 Communications Server or later, then server application instances using SHAREPORT on that stack will not work properly, and affinities for that target stack will not be communicated to the backup routing stack on failure of a primary routing stack. If a backup routing stack is not z/OS V1R5 Communications Server or later, then affinity information will not be sent to it from surviving target stacks if it takes over from a failed routing stack. Therefore, IBM strongly recommends that all TCP/IP stacks participating in distribution for a Distributed DVIPA with affinities be at least z/OS V1R5 Communications Server.
- If Sysplex Distributor routing stack is also the target stack, the affinity information in that target stack will be lost when the routing stack goes away, and the backup stack that takes over that routing stack will not have the affinity information.

Dependencies

The Sysplex Distributor routing stack must be at z/OS V1R5 Communications Server or later, as must all backup routing stacks. To maintain affinities on target stacks when the routing stack fails and a backup routing stack takes over, all target stacks must also be at z/OS V1R5 Communications Server or later. It is therefore recommended that all participating stacks be at z/OS V1R5 Communications Server or later before implementing application server affinity for a Distributed DVIPA.

What this change affects

- Availability
- Customization
- Operations
- Performance
- Usability

Using this function

If you want to take advantage of the Workload Distribution (Application Server Affinity) enhancement, perform the tasks in the following table.

Table 33. Workload Distribution (Application Server Affinity) enhancement

Task	Procedure	Reference
Enable Timed Affinity.	Add the TIMEDAFFINITY n parameter to a new or existing VIPADISTRIBUTE statement.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Display Timed Affinity setting.	Use Netstat VIPADCFG/-F to display the Timed Affinity setting.	*z/OS Communications Server: IP System Administrator's Commands*
Verify affinities (connection).	Use Netstat VCRT/-V to display the dynamic VIPA Connection Routing Table (CRT) information, using PORT filter with port filter value of 0. The DETAIL keyword can also be used with Netstat VCRT/-V to display additional Timed Affinity information for these Timed Affinity entries.	*z/OS Communications Server: IP System Administrator's Commands*
Remove Timed Affinity for future connection requests.	Specify VIPADISTRIBUTE with the TIMEDAFFINITY 0 parameter.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*

VIPABACKUP enhancement

VIPABACKUP is a statement in the VIPADYNAMIC block to designate Dynamic VIPAs (DVIPAs) to provide automatic backup when the owning stack fails. It was introduced in Communications Server for OS/390 V2R8 for cases of outages of the routing TCP/IP so that existing connections to other TCP/IPs in the sysplex are not disrupted.

In z/OS V1R5 Communications Server, VIPABACKUP is enhanced so that a DVIPA may be activated on a backup TCP/IP before it is activated elsewhere in the sysplex with the VIPADEFINE statement. The VIPABACKUP statement has new parameters that allow this to occur. A new MOVEABLE parameter, subnet mask definition, and an optional SERVICEMGR parameter can be coded on the VIPABACKUP statement in the initial profile, or in the data set referenced by a VARY TCPIP,,OBEYFILE command. The IPCS command to display the configuration is enhanced for VIPABACKUP to show the new parameters, if specified.

Restrictions

None.

What this change affects

- Availability

  This enhancement is primarily a benefit to availabilty because during the very rare Sysplex-wide IPLs, it is possible that a TCP/IP that is backup for a DVIPA is started before the TCP/IP where the DVIPA is defined with VIPADEFINE. Activating the DVIPA on the first VIPABACKUP TCP/IP for that DVIPA makes server applications available to clients outside the Sysplex more quickly than waiting for the primary TCP/IP stack and applications to be started.
- Customization
- Usability
- Operations

Using this function

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

Table 34. VIPABACKUP enhancement

Task	Procedure	Reference
Allow a DVIPA to be activated on a backup TCP/IP before it has been activated on the TCP/IP where it is defined with VIPADEFINE.	Do the following: • Add MOVEABLE IMMEDIATE or MOVEABLE WHENIDLE , the subnet mask , and optional SERVICEMGR to the VIPABACKUP statement for the DVIPA. • Add optional VIPADISTRIBUTE and VIPASMPARMS statements. • Start the backup TCP/IP stack with the updated VIPABACKUP statement in the initial profile, or issue the VARY TCPIP,,OBEYFILE command on the backup TCP/IP stack referencing the data set that contains the updated VIPABACKUP statement.	*z/OS Communications Server: IP Configuration Reference*
Verify a DVIPA setting on a backup TCP/IP.	Use Netstat VIPADCFG/-F to display a DVIPA setting on a backup TCP/IP along with other configuration information.	*z/OS Communications Server: IP System Administrator's Commands*

Dynamically assign Sysplex Distributor ports

Via APAR PQ65205, the maximum number of ports you could specify for a distributed dynamic VIPA was raised from 4 to 64. This APAR is applicable to z/OS V1R2 and z/OS V1R4. In z/OS V1R5 Communications Server, applications that are candidates for workload distribution with Sysplex Distributor, and that listen on more than 64 ports, are able to use a single distributed Dynamic VIPA by exploiting the ability to dynamically assign Sysplex Distributor ports. Previously existing applications and configurations continue to work the way they did before z/OS V1R5 Communications Server. New distributed DVIPAs configured without a PORT parameter on the VIPADISTRIBUTE statement will determine where to distribute work based on where there are applications with listening sockets bound to the distributed DVIPA, regardless of how many different ports are involved.

Restrictions

Applications must bind specifically to the designated distributed DVIPA (or have a BIND parameter configured on the PORT statement to accomplish this) and a nonzero port in order to be identified as server applications to Sysplex Distributor when no PORT statement is coded on the VIPADISTRIBUTE statement.

All TCP/IP stacks that participate in distribution in this manner (including the routing stack, backup routing stacks, and all target stacks) must be at least at the z/OS V1R5 Communications Server level.

What this change affects

- Availability
- Application development
- Operations

Some complicated applications that are candidates for workload distribution with Sysplex Distributor listen on more than four different ports. This enhancement allows a single distributed DVIPA to be used with more than four ports, simplifying the configuration of z/OS Communications Server IP, DNS, and application clients.

Using this function

If you want to dynamically assign Sysplex Distributor ports, perform the tasks in the following table.

Table 35. Dynamically assign Sysplex Distributor ports

Task	Procedure	Reference
Enable a variable number of ports for a distributed DVIPA.	Code a VIPADISTRIBUTE statement, omitting the PORT parameter.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Enable distribution of work to the application.	Configure the application to bind to the distributed DVIPA and a nonzero port for all affected listening sockets and start the application, or add a BIND parameter to the PORT reservation statements for the application.	Refer to the documentation for the application you are using. Also refer to *z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*.

DVIPA limit increase

In z/OS V1R5 Communications Server, the limit for Dynamic Virtual IP Addresses (DVIPAs) is increased from 256 to 1024. As part of this change, some TCP/IP control blocks associated with DVIPAs were moved from common storage to TCP/IP private storage.

Restrictions

The following restrictions apply:

- When defining a large number of DVIPAs, there may be a restriction involving dynamic routing using OMPROUTE. OMPROUTE currently has a limit on the number of IP addresses that may be carried in a Link State Advertisement. The limit is based on the MTU size of the network interfaces. Refer to the section on OMPROUTE in *z/OS Communications Server: IP Configuration Guide* for details of this restriction.
- If you are using both z/OS V1R5 Communications Server and pre-z/OS V1R5 Communications Server stacks in the same sysplex and they may back each other up, IBM recommends including the pre-z/OS V1R5 Communications Server stack's DVIPAs in the first 256 DVIPAs defined in the z/OS V1R5 Communications Server stack.

What this change affects

- Availability
- Application development
- Operations
- Storage

In configurations in which an application instance is associated with a DVIPA, the need for many application instances might require a large number of DVIPAs. Expanding the limit from 256 to 1024 allows you more flexibility in defining your network configuration. In addition, moving the DVIPA associated control blocks to private storage should reduce your requirement for common storage.

Using this function

If you want to take advantage of the DVIPA limit increase, perform the task in the following table.

Table 36. DVIPA limit increase

Task	Procedure	Reference
Define up to 1024 DVIPAs.	You can use a combination of the following: • VIPADEFINE statements • VIPABACKUP statements • IOCTL SIOCSVIPA DEFINEs (when the stack has a covering VIPARANGE) • BINDs (when the stack has a covering VIPARANGE) • VIPADISTRIBUTE statements, where the stack is the target	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*

Sysplexports performance enhancement

The use of the SYSPLEXPORTS function introduced in z/OS V1R4 Communications Server caused performance degradation for short-lived connections. z/OS V1R5 Communications Server provides significant performance

improvement for short-lived connections by having the stack obtain a group of ephemeral ports from the Coupling Facility (CF) and managing port allocation instead of calling the CF for each bind().

Restrictions

This performance improvement only applies to applications that bind to port 0. Applications that bind to a specific (> 1023) port will work the same as they did in z/OS V1R4 Communications Server.

What this change affects

- Performance

Using this function

This improvement is automatically implemented and does not require any action.

Integrated WLM/QoS Performance Monitor

In z/OS V1R5 Communications Server, the Policy Agent is changed to include a new performance collection function. *Performance collection* allows policy performance data to be collected and maintained for retrieval by external performance monitor applications, and also provides optional logging of the performance data to a performance log file. A Policy API (PAPI) interface is added to allow external user applications to access policy data.

Prior to z/OS V1R5 Communications Server, the Policy Based Networking functions included the following two functions related to performance of QoS policies:

- SNMP SLA subagent, which provides policy performance monitoring for the SLAPM MIB (RFC 2758).
- Sysplex Distributor (SD) Performance Monitor, which provides monitoring of network performance in relation to QoS policies installed on SD target stacks.

Performance collection in z/OS V1R5 Communications Server is another aspect of policy performance. It provides more relevant QoS performance data than the SLA subagent, allows this data to be collected and monitored in near real time by user applications through the Policy API (PAPI), and provides optional logging of the data to a performance log file for offline monitoring.

The Integrated WLM/QoS Performance Monitor API is also being used by the new Network SLAPM2 Subagent (nslapm2). This subagent provides policy performance monitoring using the NETWORK-SLAPM2-MIB. This new subagent is the replacement for the SNMP SLA subagent.

Restrictions

Applications written to the PAPI interfaces must reside on the same host as the Policy Agent.

Dependencies

Applications written to the PAPI interfaces must have access to the papiuser.h header file at compile time, to the papi.x file at bind/link edit time, and to the papi.dll at run time. Refer to *z/OS Communications Server: IP Programmer's Reference* for more information on using PAPI.

What this change affects

- Application development
- Customization

Using this function

If you want to take advantage of the integrated WLM/QoS performance monitor enhancement, perform the tasks in the following table.

Table 37. Integrated WLM/QoS performance monitor enhancement

Task	Procedure	Reference
Enable policy performance data collection.	Specify the PolicyPerformanceCollection statement in the Policy Agent configuration file for each stack for which performance collection is to be enabled.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Write or use an application to provide near real time policy performance monitoring.	Write an application using the PAPI interfaces to collect policy performance data for monitoring, or use an application written to those interfaces. A sample application is provided.	*z/OS Communications Server: IP Programmer's Reference*
Write or use an application to provide offline policy performance monitoring.	Write an application to scan the policy performance log file to collect performance data for monitoring, or use such an application. A sample application is provided.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Display policy performance data.	Issue the NETSTAT SLAP or netstat -j command to display policy performance data for policy rules.	*z/OS Communications Server: IP System Administrator's Commands*
Change automation for NETSTAT SLAP or netstat -j command.	Modify any automation tools or programs that operate on the NETSTAT SLAP or netstat -j report. The report is changed.	*z/OS Communications Server: IP System Administrator's Commands*

Increase maximum number of allowed sockets

In z/OS V1R5 Communications Server, the maximum number of sockets allowed has been increased to 65535 for the following Sockets APIs:

- Macro (EZASMI)
- Sockets Extended (EZASOKET)
- CICS Sockets (not including C Sockets under CICS)
- IMS Sockets
- REXX Sockets

Prior to z/OS V1R5 Communications Server, the highest MAXSOC value that a Sockets application could issue on an INITAPI command (or the MAXDESC value on a REXX Sockets 'Initialize' call) was 2000. The limit increase allows for a TCP socket descriptor set ranging from socket number 0 to socket number 65534.

Restrictions

This enhancement does not apply to C Sockets applications; the maximum number of sockets for C Sockets applications (for both CICS and non-CICS applications) is still 2000 in z/OS V1R5 Communications Server.

What this change affects

- Application development

Using this function

If you want to increase the maximum number of allowed sockets, perform the desired tasks in the following table.

Table 38. Increase the maximum number of allowed sockets

Task	Procedure	Reference
Determine the highest possible combined number of sockets requested by applications within a single USS process and set MAXFILEPROC to that value.	Examine the MAXFILEPROC parameter in the BPXPRMxx parmlib member and modify it (if necessary) to the optimal setting.	*z/OS UNIX System Services Planning*
For each addressing family (such as AF_INET, AF_INET6), determine the highest possible combined number of sockets in the addressing family that can be opened by all applications in the system, and specify that number as the MAXSOCKETS value.	Examine the MAXSOCKETS values in the NETWORK statements in the BPXPRMxx parmlib member and modify them (if necessary) to the optimal setting for each addressing family.	*z/OS UNIX System Services Planning*

MVS system symbol resolution enhancements in TCPIP.DATA

In z/OS V1R5 Communications Server, automatic resolution of MVS system symbols is supported for the Resolver setup file and for the TCPIP.DATA file. In previous releases, automatic resolution of MVS system symbols was not supported for the Resolver setup file or for the TCPIP.DATA file; it was necessary to use the EZACFSM1 utility program to resolve MVS system symbols for those files.

Restrictions

None.

What this change affects

- Customization

Using this function

If you want to take advantage of the enhancement for MVS system symbol resolution in TCPIP.DATA, perform the task in the following table.

Table 39. Enhancement for MVS system symbol resolution in TCPIP.DATA

Task	Procedure	Reference
Use MVS system symbols in Resolver files.	Modify the Resolver setup file and the TCPIP.DATA file to use static MVS system symbols.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Netstat enhancements

In z/OS V1R5 Communications Server, Netstat is changed in the following ways:

- The D TCPIP,,NETSTAT,ACCESS,NETWORK, Netstat CACHINFO/-C, IDS/-k, VCRT/-V, VDPT/-O, VIPADCFG/-F, VIPADYN/-v reports are enhanced to support LONG report format in preparation for future IPv6 support where applicable.
- The LONG format is further enhanced to support all of Netstat reports. The existing stack-wide output format option (FORMAT LONG/SHORT) configured on the IPCONFIG profile statement, or Netstat FORMAT/-M option, can be used to instruct all Netstat reports to produce output according to either the old or new format.
- For all of TSO NETSTAT reports, the report data do not have message identifiers displayed when the LONG format report is required. Error messages will continue to have message identifiers.
- For TSO NETSTAT HELP report, the report data do not have message identifiers displayed for both LONG and SHORT format reports.
- The new host name filter (HOSTName/-H) is added to ALL/-a, ALLCONN/-a, BYTEINFO/-b, CONN/-c, SOCKETS/-s, TELNET/-t, and VCRT/-V reports for TSO and UNIX shell Netstat.
- The existing interface filter (INTFName/-K) support is added to HOME/-h report.
- The existing IP address filter (IPAddr/-I) filter support is added to BYTEINFO/-b report.
- For all interfaces or links except VIPAs, the additional interface statistic information is added to Netstat DEVLINKS/-d report and the existing BytesIn and BytesOut are moved in the new statistics section.
- A new error message, EZZ2391I, will be issued when Netstat cannot obtain storage to retrieve requested information from the TCP/IP stack.
- The configured DELAYACKS information is added to the Configured TCP Information sections of the Netstat CONFIG/-f report.
- The LogProtoErr field is removed from the Configured TCP Information and Configured UDP Information sections of Netstat CONFIG/-f report.

Refer to *z/OS Communications Server: IP System Administrator's Commands* for a complete description of the Netstat command.

Restrictions

None.

What this change affects

- Usability
- Diagnostics
- Operations

Using this function

If you want to use the Netstat command and its enhancements, perform the task in the following table.

Table 40. Netstat enhancements

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

Intrusion Detection Services enhancements

The Intrusion Detection Services (IDS) support is enhanced to include interface flood detection as part of its ATTACK FLOOD support. This support identifies a potential interface flood condition so that an installation can take action in a timely manner. If you already have IDS policy defined for FLOODs, you will automatically receive this enhanced support.

New IDS actions, ibm-idsIfcFloodMinDiscard and ibm-idsIfcFloodPercentage, can be defined in the LDAP policy to allow you to modify the minimum number of discards and the percentage of discards that identify an interface flood. Refer to *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference* for more information.

New syslogd messages related to interface flood are added as a result of these enhancements. Refer to *z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)* for additional information.

The trmdstat flood summary and detail reports are updated to include the interface flood information. A new flood statistics report has been created to display the flood statistics data collected. Refer to *z/OS Communications Server: IP System Administrator's Commands* for more information.

The Netstat IDS/-k report has been updated to include the interface flood information. Refer to *z/OS Communications Server: IP System Administrator's Commands* for more information.

Restrictions

None.

Dependencies

For interface flood reporting, the IDS syslogd and IDS trace data in some cases provide the source MAC address of the discarded packet. In order to provide the source MAC address for discarded packets received on an OSA device in QDIO mode during interface floods, the OSA-Express microcode must support this function.

What this change affects

- Security

  Denial of service attacks often result from a malicious user flooding a system with garbage data. This support attempts to identify when this type of flood is occurring on an interface and notifies the installation.

Using this function

If your installation currently has IDS ATTACK FLOOD policy active, no action is needed to activate this support. However, if your installation does *not* have IDS ATTACK FLOOD policy active and you want to take advantage of the enhancements, you must perform the tasks in the following table.

Table 41. Intrusion Detection Services enhancements

Task	Procedure	Reference
Define IDS policies and actions.	Define Intrusion Detection policy in LDAP for the ATTACK FLOOD category.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Activate Intrusion Detection.	Start Policy Agent and TRMD. You must also start syslogd if logging or statistics are requested.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Multilevel security

In z/OS V1R5 Communications Server, TCP/IP provides support for the z/OS multilevel security environment. This environment is intended for government and commercial customers who require advanced Mandatory Access Control (MAC) security features based on security labels.

Specifically, some government and commercial installations require the advanced Mandatory Access Control (MAC) security features provided by a z/OS multilevel security environment to be extended to their TCP/IP networking environment. Beginning in z/OS V1R5 Communications Server, z/OS Communications Server TCP/IP participates in an activated z/OS multilevel security environment in several ways:

- MAC processing in stack access control and network access control is enhanced.
- Proprietary packet tagging is provided when needed between stacks on the same system or within a sysplex.
- Security labels are considered when sysplex distributor selects a target application.

Refer to the multilevel security topic in *z/OS Communications Server: IP Configuration Guide* for more information about the z/OS Communications Server support. Refer to *z/OS Planning for Multilevel Security and the Common Criteria* for concepts and overview information.

Restrictions

The following restrictions apply:

- Some z/OS Communications Server applications are restricted and others are not supported in a z/OS multilevel security environment.
- Communications between applications on two unrestricted multilevel security stacks that require a proprietary packet tag carrying a security label are restricted to XCF or IUTSAMEHOST links.
- Communications between two IP addresses that are both in security zones with a seclabel of SYSMULTI are supported only when both IP addresses are owned by z/OS V1R5 Communications Server stacks, in z/OS multilevel security environments and residing on the same z/OS system or within the same z/OS sysplex and connected with XCF.

Dependencies

The multilevel security environment support requires a z/OS V1R5 system with an active security server that provides function equivalent to RACF Security Server in

z/OS V1R5. Using the __poe() C/C++ Runtime Library Service or the SAF RACROUTE VERIFY SERVAUTH= parameter requires NETACCESS configuration in the TCPIP PROFILE.

What this change affects

- Application development
- Performance
- Customization
- Installation
- Operations
- Security

Using this function

If you want to use multilevel security, perform the task in the following table.

Table 42. Multilevel security

Task	Procedure	Reference
Enable INETD SERVAUTH Port of Entry support.	Do the following: • Define network security zones in the following ways: – Activate SERVAUTH CLASS with SETROPTS CLASSACT(SERVAUTH). – Define a NETACCESS profile for each network security zone with RDEFINE SERVAUTH. – Authorize INETD to STACKACCESS profile of each stack it will listen on with PERMIT EZB.STACKACCESS... CLASS(SERVAUTH) ID(inetd userid) ACCESS(READ). – Authorize INETD to NETACCESS profiles any client may log in from with PERMIT EZB.NETACCESS... CLASS(SERVAUTH) ID(inetd userid) ACCESS(READ). – INETD forked applications can be authorized to access all NETACCESS profiles by issuing the following command: PERMIT EZB.NETACCESS... CLASS(SERVAUTH) ID(forked process userid) ACCESS(READ). – Authorize application login users to NETACCESS profiles they may login from with PERMIT EZB.NETACCESS... CLASS(SERVAUTH) ID(login userid) ACCESS(READ). • Define datasets to have limited access by Port of Entry by doing the following: – Add/Modify profiles in DATASET CLASS with ADDSD. – Permit users to dataset profiles WHEN(SERVAUTH(...)).	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Security Server RACF Security Administrator's Guide*

OMPROUTE enhancements

z/OS V1R5 Communications Server enhances OMPROUTE in the following areas:

- The OMPROUTE detailed trace can be diverted to the CTRACE facility rather than to a file.

This enhances the performance of OMPROUTE due to synchronous file I/O during heavy OMPROUTE loads by changing these operations to memory I/O or asychronous file I/O.

- The OMPROUTE limit of 255 total interfaces is relaxed. Previously OMPROUTE could only handle 255 total interfaces on a system, including VIPA. For IPv4, OMPROUTE can now handle an unlimited number of VIPA interfaces in addition to 255 real interfaces. For IPv6, there is no absolute limit to how many interfaces OMPROUTE can handle, although performance and network design will naturally impose practical limits.
- OMPROUTE can be configured to ignore local interfaces that are not configured to it.

  The IGNORE_UNDEFINED_INTERFACES option eliminates the need to define every local interface to OMPROUTE. Without this solution, it was necessary to define every local interface to OMPROUTE whether it was being used for dynamic routing or not. If a local interface was undefined to OMPROUTE, OMPROUTE would configure it using default values, and then override stack definitions with those default values, which may be undesirable. For example, the default value for the subnet mask is the class mask and the default MTU value is 576. OMPROUTE would also possibly advertise the interface and its default values to other routers. For example, undefined interface 9.67.101.10 would be given a subnet mask of 255.0.0.0 (the class mask for a class A address) and OMPROUTE could advertise that the host could reach the entire 9.0.0.0 network via that interface. With this new function, OMPROUTE can be told to ignore interfaces not defined to it, and it will not configure or advertise those interfaces.
- The limit on multipath dynamic routes increased from 4 to 16. Previously OMPROUTE could only compute and store up to four equal cost routes to the same destination. By increasing this limit to 16, OMPROUTE's ability to implement network redundancy is greatly enhanced.
- OMPROUTE allows display of generic interfaces (which are interfaces that are not running any routing protocol), and allows OSPF MD5 authentication keys to be specified in a matter compatible with many vendor routers.
- Support for IPv6 dynamic routing is added. This includes support for IPv6 static routes, defined and learned IPv6 prefixes, and RIPng (RIP for IPv6). See "IPv6 support enhancements for OMPROUTE" on page 108 for more information.

Restrictions

The following restrictions apply when tracing to CTRACE:

- CTRACE minimum buffer size is 128k, maximum buffer size is 100 M, default buffer size is 1 M.
- Compared to previous releases, an OMPROUTE instance running with a large internal CTRACE with option DEBUGTRC active will consume more storage.
- REGION size on the OMPROUTE cataloged procedure must be at least the OMPROUTE CTRACE configured buffer size + 10 Mb.
- When the DEBUGTRC option is active, OMPROUTE debug tracing will go to CTRACE only, not to debugging files, regardless of the values of evironment variables, such as OMPROUTE_DEBUG_FILE.
- A internal CTRACE can only be accessed by dumping the OMPROUTE address space. In many cases, a matching dump with the trace is desirable, but a dump will temporarily set OMPROUTE non-dispatchable while the dump takes place.

- The new DEBUGTRC option is included in the ALL option; therefore, if you are running with the ALL option, OMPROUTE debug tracing will go to CTRACE and not to any debugging files, regardless of values of environment variables, such as OMPROUTE_DEBUG_FILE.

The following restriction is associated with relaxing the OMPROUTE limit of 255 total interfaces:

- While the number of VIPAs that can be supported by OMPROUTE is theoretically unlimited, only 255 real IPv4 interfaces (that is, interfaces on which data can actually be sent and received) are supported by OMPROUTE.

Rules for defining IPv4 Dynamic VIPA wildcards have been tightened. To define subnet mask wildcards for IPv4 dynamic VIPAs, the OSPF_INTERFACE or INTERFACE statement's IP_ADDRESS parameter must be the subnet number for the range being defined. Refer to *z/OS Communications Server: IP Configuration Reference* for additional information.

Incompatibilities

The following incompatibility is associated with relaxing the OMPROUTE limit of 255 total IPv4 interfaces:

- As the number of interfaces increases, the size of the router's link state advertisement (LSA) also increases, and there may be routers in the network that cannot accept LSAs larger than their interface MTU size, which would cause OSPF routing problems in the network.

What this change affects

- Customization

Using this function

If you want to take advantage of the general OMPROUTE enhancements, perform the tasks in the following table. If you want to take advantage of the IPv6 support enhancements for OMPROUTE, perform the desired tasks in Table 68 on page 108.

Table 43. OMPROUTE enhancements

Task	Procedure	Reference
Enable/Disable OMPROUTE tracing to CTRACE facility.	Do the following: 1. Configure the desired CTRACE buffer size in SYS1.PARMLIB(CTIORA00). 2. Change the REGION size on the OMPROUTE proc to be the CTRACE buffer size + 10 M. 3. Enable/Disable SYSTCPRT CTRACE with the new DEBUGTRC option. 4. Enable/Disable the -t and -d traces, as desired, to turn on tracing.	*z/OS Communications Server: IP Diagnosis Guide*

Table 43. OMPROUTE enhancements (continued)

Task	Procedure	Reference
Read the OMPROUTE CTRACE.	If CTRACE is directed to an internal buffer, do the following: 1. Dump the OMPROUTE address space. 2. Load the dump in IPCS and run the IPCS CTRACE formatter for component SYSTCPRT. Filter on TYPE(DEBUGTRC) to obtain the trace. If CTRACE is directed to an external writer, do the following: 1. Load the external writer output dataset in IPCS and run the IPCS CTRACE formatter for component SYSTCPRT. Filter on TYPE(DEBUGTRC) to obtain the trace.	*z/OS Communications Server: IP Diagnosis Guide*
Have more than 255 total IPv4 interfaces on the system.	None.	*z/OS Communications Server: IP Configuration Guide*
Have up to 16 dynamic routes to the same destination.	None.	*z/OS Communications Server: IP Configuration Guide*
Tell OMPROUTE to ignore any local interfaces that are not defined.	Set GLOBAL_OPTIONS IGNORE_UNDEFINED_INTERFACES=YES in the OMPROUTE configuration file.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Display IPv4 interfaces that are not running any routing protocol.	Use the DISPLAY TCPIP,tcpname,OMPROUTE,GENERIC commands.	*z/OS Communications Server: IP System Administrator's Commands*
Code OSPF MD5 authentication keys the same way they are coded in Cisco, Extreme, and other vendor routers that use a Cisco-compatible CLI.	Use the new A string method for coding authentication key.	*z/OS Communications Server: IP Configuration Reference*

TCP/IP asynchronous I/O support enhancements

In z/OS V1R5 Communications Server, the performance of asynchronous stream socket receive operations is improved when applications are changed to use common storage buffers.

Prior to this enhancement, asynchronous socket receive operations consumed more system resources than the corresponding synchronous receive operations. This enhancement reduces that disparity.

Restrictions

The use of this enhancement is restricted to authorized applications (executing in supervisor state or system key, APF-authorized, or superuser). The application must ensure that all I/O buffers are in common storage (such as ECSA or CSM-managed storage). Only the USS Callable Services Sockets API and the LE C/C++ Socket API support this enhancement.

What this change affects

- Application development
- Performance

Using this function

If you want to use the TCP/IP asynchronous I/O support enhancement, perform the task in the following table.

Table 44. TCP/IP asynchronous I/O support enhancement

Task	Procedure	Reference
Improve performance of stream socket applications using asynchronous socket I/O.	Change socket applications that issue asynchronous socket receive request to set the AioCommBuff flag in the AIOCB and ensure that all output data areas are in common storage.	*z/OS UNIX System Services Programming: Assembler Callable Services Reference* and *z/OS C/C++ Run-Time Library Reference*

Policy code restructure

In z/OS V1R5 Communications Server, the default value for the LDAP_SchemaVersion parameter on the Policy Agent ReadFromDirectory configuration statement is changed from 2 to 3.

Restrictions

None.

What this change affects

- Customization

Using this function

If you want to take advantage of the policy code restructure, perform the task in the following table.

Table 45. Policy code restructure

Task	Procedure	Reference
Examine default Policy Agent schema version and change if necessary.	If the LDAP_SchemaVersion parameter on the Policy Agent ReadFromDirectory configuration statement is not specified, verify the schema version of the policy objects defined on the LDAP server. If schema version 3 objects are defined, no action is necessary. Otherwise, specify the correct schema version on the ReadFromDirectory statement.	*z/OS Communications Server: IP Configuration Reference*

Managed System Infrastructure (msys) for Setup FTP customization support

Managed System Infrastructure (msys) for Setup was introduced in z/OS V1R2 Communications Server and enhanced in z/OS V1R4 Communications Server (see 140). In z/OS V1R5 Communications Server, complete configuration of FTP servers and FTP clients is available using msys for Setup. This allows for a GUI configuration as an alternative to creating your own configuration file.

Dependencies

msys for Setup requires the installation of the msys console on a Windows NT®, Windows XP, or Windows 2000 machine. The workstation must be connected to an up and running z/OS system using TCP/IP. The z/OS system must have msys installed, must provide TCP/IP connectivity, and must have an FTP server running. An LDAP server running on any z/OS system must be accessible.

What this change affects

- Customization
- Usability

Using this function

If you want to take advantage of the Managed System Infrastructure (msys) for Setup FTP customization support, perform the task in the following table.

Table 46. msys for Setup FTP customization support

Task	Procedure	Reference
Use the FTP configuration.	Once you install the new level of msys console, the Communications Server IP Services msys for Setup plugin will be downloaded automatically and configuration of FTP servers and clients will be available.	*z/OS Managed System Infrastructure for Setup User's Guide*

MVS Remote Execution Server support for multilevel security

In z/OS V1R5 Communications Server, the Remote Execution Server can be started with the option to add the security label to the job card.

Restrictions

None.

Incompatibilities

Existing user exits will not work correctly when the server is adding the security label to the job card. Exits need to be re-written to handle a security label on the job card if the server is run in this mode.

What this change affects

- Usability
- Operations
- Availability

- Diagnosis
- Security

Using this function

If you want to take advantage of the MVS Remote Execution Server support for multilevel security, perform the tasks in the following table.

Table 47. MVS Remote Execution Server support for multilevel security

Task	Procedure	Reference
Enable the remote execution server to communicate with clients in an multilevel security environment.	Specify the SECLABEL=Y start option in the RXSERVE procedure.	*z/OS Communications Server: IP Configuration Reference*
Migrate user exits to accommodate the security label on the job card.	Change the user exit to be able to receive the security label on the job card.	*z/OS Communications Server: IP Configuration Reference*

OSA performance enhancements

z/OS V1R5 Communications Server provides improved performance for IPv4 by offloading checksum processing to an OSA-Express in QDIO mode that supports the checksum offload function. z/OS V1R5 Communications Server also introduces new configuration parameters to provide more granular control over fixed storage usage for OSA-Express QDIO and HiperSockets interfaces, as well as some control over the inbound performance of OSA-Express QDIO interfaces.

Restrictions

In z/OS V1R5 Communications Server , the checksum offload function is only available when the OSA-Express is running in QDIO mode and only applies to IPv4 packets.

Dependencies

To use the checksum offload function, you must be running on a zSeries 990 with an Ethernet OSA-Express that supports the checksum offload function.

What this change affects

- Customization
- Performance
- Storage

Using this function

There are no tasks to enable the checksum offload function; it is automatically enabled. You may perform the optional tasks in the following table.

Table 48. OSA performance enhancements

Task	Procedure	Reference
Override the global VTAM default amount of storage for read processing for an OSA-Express or HiperSockets interface.	Specify the READSTORAGE parameter on the LINK statement for IPAQENET, IPAQTR, or IPAQIDIO and/or the INTERFACE statement for IPAQENET6.	*z/OS Communications Server: IP Configuration Reference*

Table 48. OSA performance enhancements (continued)

Task	Procedure	Reference
Control how frequently the OSA-Express adapter will interrupt the host for read processing.	Specify the INBPERF parameter on the LINK statement for IPAQENET or IPAQTR, and/or the INTERFACE statement for IPAQENET6.	*z/OS Communications Server: IP Configuration Reference*
Determine if the checksum processing is being offloaded to an OSA-Express QDIO adapter.	Inspect the NETSTAT DEVLINKS/-d output for an IPAQENET link.	*z/OS Communications Server: IP System Administrator's Commands*
Determine the amount of storage being used for read processing for an OSA-Express QDIO or HiperSockets interface.	Inspect the NETSTAT DEVLINKS/-d output for an OSA-Express QDIO or HiperSockets interface.	*z/OS Communications Server: IP System Administrator's Commands*

Improve diagnostics for DLC dumps

During recovery from a failure, the dump process may dump additional information for VTAM DLC dumps, thus requiring fewer re-creates by the user. In some cases, both VTAM and TCP/IP address spaces will be dumped. The VIT dataspace and TCP/IP CTRACE dataspace may also be included in the dump. This will provide a more useful dump.

Note: Because more information is dumped, you may need to examine the current size of your dump datasets and increase them if necessary.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

There are no exploitation actions associated with this enhancement.

DHCP daemon enhancement

The DHCP daemon will create a process ID file that can then be used in automated operations (such as a BPXBATCH job) to issue kill commands to stop the DHCP daemon.

Restrictions

None.

What this change affects

- Operations
- Usability

Using this function

If you want to issue kill commands to stop the DHCP daemon, perform the task in the following table.

Table 49. Stopping the DHCP daemon

Task	Procedure	Reference
Enable automation to stop the DHCP daemon	Issue kill -s TERM $(cat /etc/dhcpsd.*tcpipname*.pid) where *tcpipname* is the name of the TCP/IP stack with which the DHCP server established affinity. If the name of the TCP/IP stack cannot be determined, then the PID file will be named /etc/dhcpsd.INET.pid.	*z/OS Communications Server: IP Configuration Guide*

CTRACE formatting filter enhancements

Two new filters are provided when formatting SYSTCPIP CTRACE records. New selection keywords, ADDR and RECORD, can be specified on the CTRACE command OPTIONS parameter.

When ADDR is specified, only trace records containing the specified address will be formatted. When RECORD is specified, only those trace records that match the specified record number or range of numbers will be formatted.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

If you want to use the new CTRACE formatting filter enhancements, perform the tasks in the following table.

Table 50. CTRACE formatting filter enhancements

Task	Procedure	Reference
Locate SYSTCPIP trace records by control block address.	Specify CTRACE COMP(SYSTCPIP) OPTIONS((ADDR(x'hhhhhhhhh'))).	*z/OS Communications Server: IP Diagnosis Guide*
Locate SYSTCPIP trace records by record number.	Specify CTRACE COMP(SYSTCPIP) OPTIONS((RECORD(x'hhhhhhhh'))).	*z/OS Communications Server: IP Diagnosis Guide*

SMTP support for IP Mailer Name

An optional statement called IPMAILERNAME is added to the SMTPPROC configuration data set. This statement enables Simple Mail Transfer Protocol (SMTP) to forward non-local mail to the specified IP mailer name.

Restrictions

None.

What this change affects

- Customization

Using this function

If you want to use the SMTP support for IP Mailer Name, perform the task in the following table.

Table 51. SMTP support for IP Mailer Name

Task	Procedure	Reference
Enable SMTP to forward non-local mail to a specified IP mailer name.	Specify the IPMAILERNAME statement on the SMTPPROC configuration data set.	*z/OS Communications Server: IP Configuration Reference*

HiperSockets broadcast support

HiperSockets broadcast support (which is very similar to OSA-Express QDIO broadcast support) will be provided for user configured HiperSockets (iQDIO) MPCIPA devices.

Restrictions

Broadcast support is not supported for the Dynamic XCF iQDIO device.

Dependencies

You must have a system running on IBM @server zSeries 990 to use HiperSockets broadcast support.

What this change affects

- Customization

Using this function

If you want to use the HiperSockets broadcast support, perform the task in the following table.

Table 52. HiperSockets broadcast support

Task	Procedure	Reference
Enable broadcast support for user defined HiperSockets (iQDIO) devices.	If there will be applications exploiting the enhancement (using protocols which require broadcast support and using iQDIO connectivity), then configure your MPCIPA iQDIO devices (with names = IUTIQDxx) using the IPBCAST parameter on the associated IPAQIDIO LINK statement.	*z/OS Communications Server: IP Configuration Reference*

Network management

The network management interfaces provide an efficient means for network monitoring/management applications to obtain dynamic information about the run-time operation of the TCP/IP stack. Documentation on these programming interfaces can be found in *z/OS Communications Server: IP Configuration Reference*.

This function introduces the following new interfaces:

- Callable APIs for polling TCP/IP data — The new TCPIP callable API provides data for the following types of requests:
  - Active TCP connections
  - Active UDP endpoints
  - TCP listeners
  - Storage information
- Real-time asynchronous data collection interfaces:
  - Network monitor interface for capturing data packets — This interface may be used by network management tools to receive packet and data trace buffers on the TCP/IP stack.
  - Network monitor interface for obtaining TCP connection information — This interface may be used by network management tools to receive information about TCP connection activity on the TCP/IP stack.
  - Network monitor interface for obtaining real-time SMF data — This interface may be used by network management tools to receive information about FTP and TN3270 activity on the TCP/IP stack by way of SMF records.

The Real-time Asynchronous data collection interfaces are disabled by default. If you install an application that requires use of these interfaces you can activate these interfaces using the instructions in Table 53 on page 89.

Note: APARs PQ77244, PQ77837, PQ77838, and PQ77840 provide the ability to collect network management information using Network Management Interface APIs in z/OS V1R4.

Restrictions

None.

Dependencies

An AF_UNIX NETWORK statement must be configured in the BPXPRMxx parmlib member.

What this change affects

- Application development
- Operations
- Performance

Using this function

If you want to implement an application that uses the Callable API functions, review the instructions in *z/OS Communications Server: IP Programmer's Reference*.

If you want to use the Real-time asynchronous data collection interfaces, perform the desired tasks in the following table.

Table 53. Network management — Real-time asynchronous data collection interfaces

Task	Procedure	Reference

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

Enable the appropriate services on this TCP/IP stack.	Specify the parameters recommended by the network monitoring/management applications you are installing on the NETMONitor PROFILE.TCPIP statement.	*z/OS Communications Server: IP Configuration Reference*
Verify the NETMONitor setting.	Use Netstat Config/-f to display Network Monitor Configuration information.	*z/OS Communications Server: IP System Administrator's Commands*
Once these interfaces are enabled, by default, only applications that have superuser authority (access to BPX.SUPERUSER) or applications with a UID of 0 will be permitted access to these interfaces. You can further limit access to these services to specific applications through the use of RACF (or an equivalent external security manager).	Issue the following commands in the order listed: 1. SETROPTS CLASSACT(SERVAUTH) 2. SETROPTS RACLIST(REFRESH) 3. SETROPTS RACLIST(REFRESH) 4. RDEFINE SERVAUTH EZB.NETMGMT.sysname.tcpprocname. *UACC(NONE) 5. PERMIT EZB.NETMGMT.sysname.tcpprocname.*ID(*userid*) where *userid* is the client's user ID that is to be permitted. 6. SETROPTS RACLIST (REFRESH) This generic profile covers all the TCP/IP network management interfaces. Create individual profiles to attain granularity.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Implement an application that uses the Real-time asynchronous data collection interfaces.	Review the instructions in *z/OS Communications Server: IP Programmer's Reference*.	*z/OS Communications Server: IP Programmer's Reference*

Exploitation of IBM CP assist for cryptographic functions

z/OS V1R5 Communications Server supports new IBM CP assist cryptographic instructions for IPSec. The IBM @server zSeries 990 provides IBM CP assist that improves symmetric encryption/decryption performance, as well as SHA1 performance. These instructions are synchronous clearkey.

Some zSeries 990s support a new cryptographic coprocessor, called the PCIX Cryptographic Coprocessor (PCIXCC). However, IPSec will attempt encryption/decryption first by using the new ICSF crypto assist instructions; and if crypto assist is not present, IPSec will attempt encryption/decryption using PCIXCC. If PCIXCC is not available or fails, IPSec will perform encryption/decryption by using software.

Table 54. Encryption/decryption methods and the zSeries 990

Encryption/decryption method	zSeries 990 without PCIXCC feature	zSeries 990 with PCIXCC feature
Crypto assist	IPSec invokes crypto assist if present.	IPSec invokes crypto assist if present.
PCIXCC	Not available.	If crypto assist is not present, IPSec invokes PCIXCC.
Software	If crypto assist is not present or if it fails, IPSec invokes software.	If PCIXCC is not present or if it fails, IPSec invokes software.

What this change affects

- Performance

Using this function

There are no required actions to exploit the IBM CP assist for cryptographic functions.

IBM @server zSeries 990 HiperSockets enhancements

HiperSockets were introduced in z/OS V1R2 Communications Server. In z/OS V1R5 Communications Server, the following HiperSockets enhancements are available with and exclusive to the IBM @server zSeries 990:

- Spanned channels

  With the introduction of a new Channel SubSystem, transparent sharing of Internal Coupling Channels (ICs) and HiperSockets is possible.

  The Multiple Image Facility (MIF) allows sharing of channel resources across LPARs. ICs and HiperSockets can be configured as MIF spanning channels. *Spanning channels* is the ability for Internal Coupling Channels and HiperSockets channels to be configured to multiple Channel SubSystems, and be transparently shared by any or all of the configured LPARs without regard to the Logical Channel SubSystem to which the LPAR is configured. This support is applicable to Internal Coupling Channels (ICP CHPID type) for Parallel Sysplex and to HiperSockets (IQD CHPID type).
- Increased number of HiperSockets CHPIDs (iQDIO Internal LANs)

  The number of Internal LANs that can be configured is increased from 4 to 16.

  When HiperSockets was introduced, up to 4 internal Local Area Networks (LANs) could be configured. An IQD CHPID represents one Internal LAN. That number is now increased to up to 16 internal LANs (IQD CHPIDs).
- Increased number of supported TCP/IP stacks

  The number of supported TCP/IP stacks is increased from 1024 to 4096. Because each TCP/IP stack requires one communication queue, this means 4096 TCP/IP stacks are now supported (instead of 1024 TCP/IP stacks).

  A HiperSockets channel must be spanned in order to communicate between LPARs in different LCSSs.

Restrictions

None.

Dependencies

These HiperSockets enhancements are exclusive to the IBM @server zSeries 990.

Using this function

The HiperSockets enhancements are fundamentally transparent to Communications Server. There are no Communications Server configuration actions required (there are no changes in VTAM or TCP/IP definitions). If you want to take advantage of the enhancements, however, you must consider which Logical Partitions (LPs) will be required to connect (span) across LCSS (Logical Channel Subsystems). Next, you must decide how to deploy the IQD CHPID spanning.

The TCP/IP Dynamic XCF support will dynamically attempt to use HiperSockets connectivity and can dynamically detect if the sysplex IQD CHPID was configured to span across LCSSs. IQD CHPIDs and the CHPID's spanning attributes are configured using HCD. Refer to *z/OS HCD User's Guide* for configuration details.

If you want to use IBM @server zSeries 990 HiperSockets enhancements, perform the task in the following table.

Note: There are no changes required in VTAM or TCP/IP definitions.

Table 55. IBM @server zSeries 990 HiperSockets enhancements

Task	Procedure	Reference
Determine if spanning IQD CHPIDs should be deployed in your IBM @server zSeries 990.	Consider if your IBM @server zSeries 990 will be configured into MCSSs (Multiple Channel SubSytems). If applicable, determine if there are Logical Partitions in different LCSSs that will require internal connectivity using HiperSockets (using IQD CHPID spanning). Using HCD, configure your IQD CHPID to span to the appropriate LCSSs.	*z/OS HCD User's Guide*

IPv6 support enhancements

z/OS V1R4 Communications Server introduced support for both IPv4 and IPv6 IP addresses for certain functions and applications; see "IPv6 support" on page 148 for the exploitation details of that release, including information about enabling and configuring IPv6.

Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for general information about the design, concepts, and enablement considerations of using IPv6 support.

In z/OS V1R5 Communications Server, the support for IPv6 addressing is enhanced in many ways. These enhancements and exploitation considerations are described in the following sections:

- "IPv6 support — Full Virtual LAN (VLAN) support for OSA-Express" on page 92
- "IPv6 support for Enterprise Extender" on page 93
- "IPv6 support and upgrade for Sendmail" on page 93
- "IPv6 support for CICS sockets API" on page 98
- "IPv6 support for Policy" on page 101

IPv6 support — Full Virtual LAN (VLAN) support for OSA-Express

z/OS V1R5 Communications Server extends Virtual LAN support by allowing you to assign a Virtual LAN identifier (VLAN ID) to an OSA-Express link or interface. This allows all packets using an OSA-Express to carry a VLAN ID, and thus segregate traffic into different Virtual LANs without needing multiple real LANs or creating new subnetworks.

See "Full Virtual LAN support for OSA-Express" on page 64 for the restrictions, dependencies, and incompatibilities that you must consider when using the VLAN ID support **for either IPv4 or IPv6 traffic**. See Table 31 on page 65 for the exploitation task associated with using the VLAN ID support for IPv4 traffic. The exploitation task associated with using IPv6 traffic follows.

Restrictions

The VLANID parameter of the DEVICE, LINK, and INTERFACE statements interacts with the PRIRouter and SECRouter parameters. If you configure both a VLANID and either PRIRouther or SECRouter, then this TCP/IP instance will act as a router for this VLAN (ID) only. Datagrams that are received at this device for an unknown IP address will only be routed to this TCP/IP instance if it is VLAN tagged with this VLAN ID. For additional information regarding how VLANID interacts with PRIRouting, refer to *z/OS Communications Server: IP Configuration Reference*.

Using this function

If you want to take advantage of full Virtual LAN support for IPv6 traffic, perform the task in the following table.

Table 56. Full Virtual LAN (VLAN) support for IPv6 traffic

Task	Procedure	Reference
Specify the Virtual LAN identifier desired **for IPv6 traffic** through an OSA-Express interface.	Define the VLANID keyword on the INTERFACE statement representing this OSA-Express. This may be the same or may be different from the VLAN ID for IPv4 traffic.	*z/OS Communications Server: IP Configuration Reference*

IPv6 support for Enterprise Extender

In z/OS V1R5 Communications Server, the support for Enterprise Extender (EE) is enhanced to be IPv6 enabled. It is also enhanced to allow you to specify a hostname when using either IPv4 or IPv6 addressing; see "Enterprise Extender enhancements" on page 65 for more information. Refer to "Enterprise Extender enhancements" on page 205 for details of the z/OS V1R5 Communications Server Enterprise Extender enhancements, including restrictions, incompatibilities, and exploitation procedures.

IPv6 support and upgrade for Sendmail

z/OS UNIX Sendmail is a mail program running in an UNIX System Services shell. It has function similar to SMTPROC known in previous MVS TCP/IP versions but allows HFS access, mail filters, TLS connections, and IPv6 socket support. However, if you intend to use the mail server also as a gateway to an NJE/RSCS network, the SMTPROC server has to be used instead of the Sendmail daemon because of rewriting the mail header for NJE/RSCS networks or vice versa. The Sendmail program Version 8.12.1 is based on the Berkeley UNIX 4.1c BSD code.

z/OS V1R5 Communications Server is enhanced in the following areas:

- IPv6 support

  IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4). The most significant change from IPv4 to IPv6 is the "Expanded Addressing Capabilities." Thus, it affects the IP resolving.

- TLS support

  This is an extension to the SMTP service that allows an SMTP server and client to use transport-layer security to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

- Mail filter support

  The Sendmail Mail Filter API (Milter) is designed to allow third-party programs access to mail messages as they are being processed in order to filter meta-information and content.

- Configuration and file location

  Sendmail configuration changed due to many new features. Those changes include configuration file's version number and header format, for example. You can modify old sendmail.cf (8.8.7) to let it be parsed by Sendmail (8.12.1) correctly. See Table 58 on page 95 for the steps to take.

  Sendmail 8.9 has introduced a new configuration directory for Sendmail related files, /etc/mail.Beginning with 8.10, all files will use this directory by default (some options may be set by OSTYPE() files). This new directory should help to restore uniformity to Sendmail's file locations.

  See Table 57 on page 94 for some of the common changes.

- SAF (security authorization facility)

  In z/OS V1R5, Sendmail introduced separate configuration files for the MTA and the MSP, /etc/mail/sendmail.cf and /etc/mail/submit.cf. This was done to isolate authority and increase security. But it now requires that the two ways of executing Sendmail have their SAF configured.

Table 57. Sendmail changes in z/OS V1R5 Communications Server: Old filenames and new filenames

Old filename	New filename
/etc/bitdomain	/etc/mail/bitdomain
/etc/sendmail.cf	/etc/mail/sendmail.cf /etc/mail/zOS.cf
/etc/domaintable	/etc/mail/domaintable
/etc/genericstable	/etc/mail/genericstable
/etc/uudomain	/etc/mail/uudomain
/etc/virtusertable	/etc/mail/virtusertable
/etc/userdb	/etc/mail/userdb
/etc/aliases	/etc/mail/aliases
/etc/sendmail/aliases	/etc/mail/aliases
/etc/ucbmail/aliases	/etc/mail/aliases
/usr/adm/sendmail/aliases	/etc/mail/aliases
/usr/lib/aliases	/etc/mail/aliases
/usr/lib/mail/aliases	/etc/mail/aliases
/usr/ucblib/aliases	/etc/mail/aliases
/etc/sendmail.cw	/etc/mail/local-host-names
/etc/mail/sendmail.cw	/etc/mail/local-host-names
/etc/sendmail/sendmail.cw	/etc/mail/local-host-names
/etc/sendmail.ct	/etc/mail/trusted-users
/etc/sendmail.oE	/etc/mail/error-header
/etc/sendmail.hf	/usr/lib/sendmail.hf
/etc/mail/sendmail.hf	/usr/lib/sendmail.hf
/usr/ucblib/sendmail.hf	/usr/lib/sendmail.hf
/etc/ucbmail/sendmail.hf	/usr/lib/sendmail.hf
/usr/lib/sendmail.hf	/usr/lib/sendmail.hf
/usr/share/lib/sendmail.hf	/usr/lib/sendmail.hf
/usr/share/misc/sendmail.hf	/usr/lib/sendmail.hf
/share/misc/sendmail.hf	/usr/lib/sendmail.hf
/etc/service.switch	/etc/mail/service.switch
/etc/sendmail.st	/etc/mail/statistics
/etc/mail/sendmail.st	/etc/mail/statistics
/etc/mailer/sendmail.st	/etc/mail/statistics
/etc/sendmail/sendmail.st	/etc/mail/statistics
/usr/lib/sendmail.st	/etc/mail/statistics
/usr/ucblib/sendmail.st	/etc/mail/statistics
old /etc/bitdomain	/etc/mail/bitdomain
/etc/sendmail.cf	/etc/mail/sendmail.cf and /etc/mail/zOS.cf
/etc/domaintable	/etc/mail/domaintable
/etc/genericstable	/etc/mail/genericstable

Notes:

1. All of the paths shown in Table 57 on page 94 actually use a new m4 macro MAIL_SETTINGS_DIR to create the pathnames. The default value of this variable is /etc/mail/. If you set this macro to a different value, you MUST include a trailing slash.
2. All filenames used in a .mc (or .cf) file should be absolute (starting at the root, for example, with /). Relative filenames can produce unpredictable results during operations (unless otherwise noted).

New Sendmail external interfaces

There are new interfaces for Sendmail in z/OS V1R5 Communications Server. Refer to *z/OS Summary of Message and Interface Changes* for more information about these interfaces.

Sendmail 8.12.1 adds support for mail filter APIs. For a complete description of these APIs, refer to *z/OS Communications Server: IP Programmer's Reference*.

Restrictions

None.

Dependencies

At least one TCP/IP stack must be available. A DNS server may be needed if name server MX lookup is used. A Certificate Authority (CA) server may be needed to issue certificates and an LDAP server may be needed to store certificates if TLS support is used.

What this change affects

- Customization
- Operation
- Security

Using this function

If you want to use the Sendmail enhancements, perform the desired tasks in the following tables.

Table 58. Sendmail enhancements

Task	Procedure	Reference
Use IPv6 support — Configure Sendmail to listen on an IPv6 port.	Perform the following steps: 1. Ensure the TCP/IP stack is IPv6-enabled. 2. Add DAEMON_OPTIONS to sendmail.mc. 3. Use m4 to create sendmail.cf. 4. Check DaemonPortOptions in sendmail.cf.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Table 58. Sendmail enhancements (continued)

Task	Procedure	Reference
Use TLS support — Configure Sendmail to use TLS with a gskkyman database.	Perform the following steps: 1. Get the CA for client and/or server from your network administrator. 2. Copy /usr/lpp/tcpip/samples/sendmail/cf/zOS.cf to /etc/mail/zOS.cf. 3. Set KeyfilePath to the path for the gsk key information. 4. Set ServerKeyfile and ServerPWFile for the kdb and stash file information used when Sendmail is used as a server. 5. Set ClientKeyfile and ClientPWFile for the kdb and stash file information used when Sendmail is used as a client. 6. Optionally set the CipherLevel to the SSLV3/TLS cipher to be used.	*z/OS Crytographic Service System Secure Sockets Layer Programming*
Configure Sendmail to use filters.	Perform the following steps: 1. Write the user written mail filter program. 2. Edit sendmail.mc to add MAIL_FILTER and INPUT_MAIL_FILTER features. 3. Issue m4 command to generate sendmail.cf.	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Communications Server: IP Programmer's Reference*
Use configuration and file location support — Create new sendmail.cf.	Perform the following steps: 1. Copy /usr/lpp/tcpip/samples/sendmail/cf/sample.mc to sendmail.mc. 2. Edit sendmail.mc to add needed features. 3. Issue m4 command to generate sendmail.cf.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Use configuration and file location support for Mail Submission Program (MSP)	Perform the following steps: 1. Copy /usr/lpp/tcpip/samples/sendmail/cf/submit.mc to a private copy of submit.mc. 2. Edit submit.mc to add any needed features. 3. Issue m4 command to generate submit.cf.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Table 58. Sendmail enhancements (continued)

Task	Procedure	Reference
Use configuration and file location support — Migrate sendmail.cf.	Although old configuration files can be used in this version, Sendmail will display a warning message. It is difficult to manually edit old sendmail.cf to take full advantage of new features. Therefore, IBM recommends that you use the m4 preprocessor to generate sendmail.cf, then make necessary modification, as follows: 1. Check old sendmail.cf's comment (at the beginning of the file) to spot those features used by old Sendmail. 2. Add those features in .mc file. 3. Issue m4 command to generate .cf file. 4. Compare the old and new sendmail.cf to find subtle difference. 5. Edit new sendmail.cf manually to complete the migration. Another way to migrate an 8.8.7 sendmail.cf file to 8.12.1 when the corresponding mc file is missing is to start with the old version of Sendmail. Follow these steps: 1. Generate a sample.cf file from the sample.mc.. 2. Diff the old sendmail.cf file and sample.cf with the command: "diff -w sendmail.cf sample.cf". 3. Check diff output for features in the old sendmail.cf that are not in sample.cf. 4. Modify sample.mc to contain features present in old sendmail.cf not present in sample.cf. 5. Generate a new sample sample.cf based on the modified sample.mc. 6. Repeat steps 3 - 6 until sendmail.cf and sample.cf are the same. You can choose to use the new version of Sendmail. Follow these steps: 1. Use the sample.mc file created in step 5 and add in any Sendmail 8.12.1 options to be used. 2. Generate a new sendmail.cf from the sample.mc with any new Sendmail 8.12.1 options to be used.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Table 58. Sendmail enhancements (continued)

Task	Procedure	Reference
Use configuration and file location support — Migrate ancillary files (location).	aliases => compatible, relocation proposed /etc/mail/aliases aliases.dir, aliases.pag => rebuild with aliases /etc/mail/aliases.dir /etc/mail/aliases.pag sendmail.cw => compatible, rename proposed /etc/mail/local-host-names sendmail.ct => compatible, rename proposed /etc/mail/trusted-users sendmail.oE => compatible, rename proposed /etc/mail/error-header sendmail.st => recreate with following steps 1. cp /dev/null /etc/mail/statistics 2. chmod 644 /etc/mail/statistics bitdomain => compatible, relocation proposed /etc/mail/bitdomain domaintable =>compatible,relocation proposed /etc/mail/domaintable genericstable =>compatible,relocation proposed /etc/mail/genericstable uudomain => compatible, relocation proposed /etc/mail/uudomain virtusertable => compatible, relocation proposed /etc/mail/virtusertable userdb => compatible, relocation proposed /etc/mail/userdb service.switch =>compatible,relocation proposed /etc/mail/service.switch	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Configure Sendmail MTA and MSA SAF authority user IDs.	Perform the steps as described in EZARACF sample in SEZAINST to add the MAILNULL, SMMSP, and SENDMAIL user IDs along with the SMMSPGRP and SNDMGRP group.	*z/OS Communications Server: IP Configuration Guide*

IPv6 support for CICS sockets API

z/OS V1R5 Communications Server enables IP CICS sockets to support IPv6. This includes the following changes:

- The Task Related User Interface is enabled to define standard and enhanced IPv6 Listeners/subtasks.
- The IBM distributed Listener is enabled to support IPv6 enabled child subtasks.
- The IP CICS Advanced Sockets API is affected as follows:
  - It is enabled to support IPv6 functions.
  - It has new socket options.
  - It has new ioctl commands.
  - It has new resolver functions.
  - It has new utility functions.
- The IP CICS C Sockets API will be affected as follows:
  - It is enabled to support IPv6 functions.
  - It has new socket options.
  - It has new ioctl commands.
  - It has new resolver functions.

– It has new utility functions.

Refer to *z/OS Communications Server: IP CICS Sockets Guide* for more information about IPv6 support for CICS sockets API. Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* to become familiar with IPv6 concepts.

DNS/WLM migration considerations

DNS/WLM continues to support CICS Listeners desiring to participate in workload balancing for IPv4 clients and IPv6 clients. IPv6-enabled Listeners are still able to participate in workload balancing for their IPv4 clients and IPv6 clients. IPv6 clients connecting to IPv6 Listeners participating in DNS/WLM must connect using an IPv4-mapped IPv6 address. DNS/WLM only returns an IPv4 address. IPv6 clients should use unique hostnames and DNS entries should be made to allow unique host names to exist in different DNS zones to enable an IPv6 client to get an AAAA address to use when connecting to an IPv6-enabled Listener.

Restrictions

None.

Incompatibilities

The EZACICAL CICS sockets API is not IPv6 enabled.

Dependencies

You must be running on an IPv6-enabled stack if you have IPv6-enabled Listeners.

What this change affects

- Application development
- Customization
- Diagnosis
- Installation
- Operations

Using this function

If you want to use the IPv6 support for CICS sockets API, perform the desired tasks in the following table.

Table 59. IPv6 support for CICS sockets API

Task	Procedure	Reference
Define TCP/IP stacks being used by the IP CICS interface as IPv6.	Add an AF_INET6 NETWORK statement to your BPXPRMxx SYS1.PARMLIB member.	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Communications Server: IPv6 Network and Application Design Guide*
Define an IPv6 Listener.	Either configure a Listener as IPv6 through the use of the AF=INET6 operand of the EZACICD assembler macro or by changing the AF entry on the EZAC ALTER screen to INET6. The EZAC BMS maps are modified to support the AF=INET|INET6 entry for the ALTER, CONVERT, DEFINE and DISPLAY Listener.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IPv6 Network and Application Design Guide*

Table 59. IPv6 support for CICS sockets API (continued)

Task	Procedure	Reference
Add or remove WLM Groups from the Listener definition.	Do one of the following: • Use the EZACICD TYPE=Listener macro to add, change or remove the entry on the WLMGN1, WLMGN2, or WLMGN2 operands. • Use the EZAC CICS transaction and specify the ALTER command to change the values for the WLM Groups.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IPv6 Network and Application Design Guide*
Configure the CICS Domain Name Server Cache.	Create a Bind9/DNS Caching only server so that the CICS Domain Name Server Cache is enabled to support IPv6 names.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IP Configuration Guide*
Update Child server programs to handle IPv6 Transaction Initiation Message (Listener Output Format).	Change programs to use the IPv6 format of the socket address structure contained in the Transaction Initiation Message (Listener Output Format) for both the STANDARD and ENHANCED Listener.	*z/OS Communications Server: IP CICS Sockets Guide*
Update Security/Transaction Link Module for the Listener.	Adjust the CICS Commarea so that it contains the Connecting clients IP address, address family, the Listener IP address, and address family.	*z/OS Communications Server: IP CICS Sockets Guide*
Create or change user developed Listener sockets programs to IPv6.	Change the socket address structures from IPv4 to IPv6. Change the domains/address families from AF_INET to AF_INET6.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IPv6 Network and Application Design Guide*
Create or change child server application sockets programs to IPv6.	Change the socket address structures from IPv4 to IPv6. Change the domains/address families from AF_INET to AF_INET6.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IPv6 Network and Application Design Guide*
Resolve IPv6/IPv4 addresses from host and/or service names.	Convert IP CICS Sockets program containing a GETHOSTBYNAME to issue a GETADDRINFO and a FREEADDRINFO.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IPv6 Network and Application Design Guide*
Resolve host and/or service names from socket addresses.	Convert IP CICS Sockets programs containing a GETHOSTBYADDR to issue a GETNAMEINFO.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IPv6 Network and Application Design Guide*
Verify Resolver functions.	Resolver trace messages can be captured for resolver function executed by IP CICS Sockets program by adding a TRACE RESOLVER statement to the TCPDATA file in the TCPPARMS dataset or by adding a SYSTCPT DD card to the CICS job deck.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IP Diagnosis Guide*
Use IPv6 Multicast.	Convert IP CICS Sockets programs that use IPv4 multicast socket options to the IPv6 multicast socket options.	*z/OS Communications Server: IP CICS Sockets Guide* and *z/OS Communications Server: IPv6 Network and Application Design Guide*

Table 59. IPv6 support for CICS sockets API (continued)

Task	Procedure	Reference
Adjust message automation, if necessary.	Change NetView message processing facility exits to accommodate either IPv4 or IPv6 addresses. Note that IP CICS Sockets messages will display either an IPv4 or an IPv6 IP address of the connecting client.	*z/OS Communications Server: IP CICS Sockets Guide*
Convert the addrinfo structure.	Use the EZACIC09 callable program to expand the fields from the addrinfo structures returned from a GETADDRINFO call. Programs that call EZACIC09 must concatenate *hlq*.SEZATCP to the SYSLIB Linkage Editor step. This will ensure the program will be found.	*z/OS Communications Server: IP CICS Sockets Guide*

IPv6 support for Policy

In z/OS V1R5 Communications Server, the Policy Agent is changed to support IPv6 addresses in policy definitions. Prior to z/OS V1R5 Communications Server, the Policy Agent only supported IPv4 addressing.

In addition, the Policy Agent LDAP schema definition files are updated to include changes for IPv6 support. Intrusion Detection Services (IDS) policy has been changed to include support for interface flood detection.

Restrictions

None.

Dependencies

To support IPv6 addresses, the TCP/IP stack must be enabled for IPv6.

What this change affects

- Customization
- Installation

Using this function

If you want to use the IPv6 support for Policy, perform the tasks in the following table.

Table 60. IPv6 support for Policy

Task	Procedure	Reference
Modify Policy Agent policy rules as needed to include IPv6 addresses. **Note:** IPv6 is not supported for Intrusion Detection Services rules and actions in z/OS V1R5 Communications Server.	Specify IPv6 source or destination addresses, or inbound or outbound interfaces, for policy rules defined in configuration files or on an LDAP server. Interfaces can now be specified by interface name, as well as IPv4 interface address.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Modify Policy Agent subnet priority ToS masks as needed to include IPv6 interfaces.	Subnets can now be specified by interface name as well as IPv4 interface address.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Change automation for pasearch command display output if necessary.	Modify any automation tools or programs that operate on the pasearch command output. The display output is changed.	*z/OS Communications Server: IP System Administrator's Commands*

Table 60. IPv6 support for Policy (continued)

Task	Procedure	Reference
Change automation for Policy Agent messages if necessary.	Modify any automation tools or programs that operate on messages EZZ8446I, EZZ8449I, EZZ8450I, or EZZ8451I. These have been replaced with EZZ8775I, EZZ8776I, EZZ8777I, and EZZ8778I, respectively.	*z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)*
Update LDAP schema definitions when migrating from Communications Server for OS/390 V2R10.	Install the following set of LDAP schema definition files on the LDAP server, in the following order: pagent_v3schema.ldif pagent_idsschema.ldif pagent_schema_r5updates.ldif	*z/OS Communications Server: IP Configuration Guide*
Update LDAP schema definitions when migrating from z/OS V1R2 or V1R4 Communications Server.	Install the following LDAP schema definition file on the LDAP server: pagent_schema_r5updates.ldif	*z/OS Communications Server: IP Configuration Guide*

IPv6 support for the SYSLOG daemon and the DCAS, TFTP, and SNTP servers

z/OS V1R5 Communications Server enhances the SYSLOG daemon and DCAS, TFTP, and SNTP servers so that they can operate with IPv6 networks.

In addition, once you have permitted RACF to allow the SYSLOG daemon to run in a non-swappable state, it becomes the default for the SYSLOG daemon. Prior to z/OS V1R5 Communications Server, if the system became busy, it was possible that the SYSLOG daemon's address space was swapped out. This could have prevented messages from being logged or could have delayed the logging of messages.

Furthermore, in z/OS V1R5 Communications Server the stratum level used by the SNTP daemon can be specified with a start option. The stratum level is an indication of the accuracy of the z/OS clock. This may vary from site to site. The default stratum level is 1.

Restrictions

None.

Incompatibilities

To support IPv6 addresses, the TCP/IP stack must be enabled for IPv6.

Dependencies

An IPv6 enabled TCP/IP stack, such as z/OS V1R5 Communications Server TCP/IP configured as an AF_INET6 network, is required for the new IPv6 function.

What this change affects

- Availability
- Operations
- Diagnosis
- Usability

Using this function

If you want to use the IPv6 support for the SYSLOG daemon and the DCAS, TFTP, and SNTP servers, perform the tasks in the following table.

Table 61. IPv6 support for the SYSLOG daemon and the DCAS, TFTP, and SNTP servers

Task	Procedure	Reference
Enable SYSLOG daemon and DCAS, TFTP, and SNTP servers to communicate with IPv6 nodes as well as IPv4 nodes.	Configure z/OS TCP/IP (or any other TCP/IP stack) as an AF_INET6 network.	*z/OS Communications Server: IPv6 Network and Application Design Guide*
Make syslogd run in a non-swappable state.	Configure your security product (such as RACF) to allow the SYSLOG daemon to run as non-swappable.	*z/OS Communications Server: IP Configuration Guide*
Make syslogd run in a swappable state.	Configure your security product (such as RACF) to allow the SYSLOG daemon to run as swappable.	*z/OS Communications Server: IP Configuration Guide*
Specify the SNTPD's stratum level.	Use the -s start option with a value of 1-15.	*z/OS Communications Server: IP Configuration Reference*

IPv6 support for TSO rexec and rsh and associated MVS daemons

z/OS V1R5 Communications Server enhances the TSO rexec and rsh commands and RXSERVE so that they can operate over IPv6 networks. Support has been added for the rsh command in the UNIX environment.

Restrictions

None.

Incompatibilities

Existing user exits will not work correctly when the server is using IPv6 sockets and true IPv6 clients connect. Exits need to be re-written to handle an IPv6 socket address structure if the server is run in this mode.

Dependencies

To take advantage of the IPv6 support offered by the TSO rexec and rsh commands, the MVS rexec/rsh server, and the z/OS UNIX rsh command, the TCP/IP stack on your system must support IPv6 networking. If not, these applications will operate in IPv4 mode.

What this change affects

- Availability
- Operations
- Diagnosis
- Usability

Using this function

If you want to use the IPv6 support for TSO rexec and rsh and associated MVS daemons, perform the tasks in the following table.

Table 62. IPv6 support for TSO rexec and rsh and associated MVS daemons

Task	Procedure	Reference
Enable the TSO rexec and rsh commands and the MVS rexec/rsh server and the UNIX rsh command to communicate with IPv6 nodes as well as IPv4 nodes.	Configure z/OS TCP/IP (or any other TCP/IP stack) as an AF_INET6 network.	*z/OS Communications Server: IPv6 Network and Application Design Guide*
Preserve operation of user exits that do not support IPv6.	Specify the IPV6=N start option in the RXSERVE procedure.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Migrate user exits to operate with IPv6 clients.	Change the user exit to be able to receive an IPv6 socket address structure.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

IPv6 support for SMF recording

z/OS V1R5 Communications Server enhances the existing use of System Management Facilities (SMF) to provide additional information for system management and accounting. Specifically, the SMF recording enhancements include the following:

- IPv6 enablement of SMF records is complete.
  - IPv6 and ICMPv6 statistics are reported in the TCP/IP Statistics record.
  - A stack's IPv6 enablement status is reflected in the Stack Initialization and Termination records.
  - Statistics for IPv6 interfaces are reported in the Interface Statistics record.
  - IPv6 TN3270 connections are reflected in the TN3270 Server Session Initialization and Termination records.
- Security information is added to the various FTP server and client SMF records, for the purpose of identifying the security mechanism and levels for FTP transfers.
- The TCP Connection Termination record is modified to report Telnet-specific information, such as LU name, application name, and protocol, for those connections that are TN3270 connections.
- The formats for several of the type 119 SMF records are changed to add additional subsections reflecting new information.

Refer to *z/OS Communications Server: IP Configuration Reference* for the specific details.

Restrictions

None.

What this change affects

- Operations

Using this function

If you want to use the IPv6 support for SMF recording, perform the task in the following table.

Table 63. IPv6 support for SMF recording

Task	Procedure	Reference
Update SMF processing tools.	Update any automated SMF processing tools to make use of the additional information now provided. Utilize EZASMF77 to get the correct mappings of the changes.	*z/OS Communications Server: IP Configuration Reference*

IPv6 support for XCF, SameHost, and ESCON

In z/OS V1R5 Communications Server, the multipath channel point-to-point (MPCPTP) Data Link Control (DLC) is updated to support IPv6 traffic. With the new support, a new interface type (MPCPTP6) may be used to carry IPv6 traffic over ESCON® channels, over XCF links in a sysplex, or between z/OS Communications Server images using the virtual channel to channel (CTC) simulated by the IUTSAMEH function in VTAM.

The MPCPTP6 interface may point to the same TRLE as an MPCPTP DEVICE, thus allowing IPv4 and IPv6 traffic to share the same physical resources.

Prior to this enhancement, the only network attachment supported for IPv6 traffic was the OSA-Express.

The Netstat DEVLINKS/-d displays are changed to describe the MPCPTP6-type interface.

Restrictions

The following restrictions apply:

- Interface type MPCPTP6 may only be used with z/OS V1R5 Communications Server or above.
- A mix of static and dynamic IPv4 and IPv6 definitions for a device is not allowed. For example, if a static IUTSAMEH IPv4 device and link is defined, an IPv6 dynamic definition for IUTSAMEH will not be created. If a static IUTSAMEH IPv6 interface is defined, an IPv4 dynamic definition for IUTSAMEH will not be created. The same logic also applies for XCF links; a mix of static and dynamic IPv4 and IPv6 definitions is not allowed for an XCF link.

What this change affects

- Customization
- Usability

Using this function

If you want to use IPv6 support for XCF, SameHost, and ESCON, perform the tasks in the following table.

Table 64. IPv6 support for XCF, SameHost, and ESCON

Task	Procedure	Reference
Configure an MPC point-to-point interface to carry IPv6 traffic.	Code an MPCPTP6 interface statement.	*z/OS Communications Server: IP Configuration Reference*
START or STOP an MPC point-to-point interface for IPv6 traffic.	Use START/STOP commands.	*z/OS Communications Server: IP Configuration Reference*
Monitor interface status and statistics.	Use Netstat DEVLINKS/-d commands.	*z/OS Communications Server: IP System Administrator's Commands*

IPv6 support enhancement for IPAQENET6 Interface type

In z/OS V1R5 Communications Server, the IPAQENET6 Interface type, which handles IPv6 over Ethernet/QDIO, is enhanced to allow for manual configuration of the Interface ID portion of local IPv6 addresses.

In z/OS V1R4 Communications Server, network administrators had no control over the Interface ID portion (bits 64 through 128) of Link-Local or Autoconfigured IPv6 addresses on their IPAQENET6 interfaces. Without control over the Interface ID value, the possibility exists that multiple IPv6 hosts in a customer network will have the same IPv6 address. With the z/OS V1R5 Communications Server support, customers who wish to have unique IPv6 addresses in the Link, Site, and Global scopes can manually configure unique Interface IDs onto their IPAQENET6 interfaces. This will then result in formation of unique Link-Local, Site-Local, and Global IPv6 addresses.

Restrictions

None.

What this change affects

- Customization
- Usability

Using this function

If you want to use IPv6 support for IPAQENET6 Interface type, perform the task in the following table.

Table 65. IPv6 support for IPAQENET6 Interface type

Task	Procedure	Reference
Optionally configure the IPv6 Interface ID for your IPAQENET6 and/or MPCPTP6 interfaces. This may be useful if other IPv6 nodes need to define static routes to this host, or if you use IPv6 addresses in Multilevel Security policies. **Note:** If you do not manually configure the Interface ID, the system will select an Interface ID for you, using either a random value (on an MPCPTP6 interface), or a value derived from the MAC address (on an IPAQENET6 interface).	Code the INTFID keyword on your IPAQENET6 and/or MPCPTP6 interfaces.	*z/OS Communications Server: IP Configuration Reference*

IPv6 support for dynamic XCF

z/OS V1R4 Communications Server introduced the basic support of IPv6 addresses on the TCPIP stack, but that support did not include static or dynamic XCF. z/OS V1R5 Communications Server provides IPv6 support for static and dynamic XCF. This section describes the IPv6 support for dynamic XCF. See "IPv6 support for XCF, SameHost, and ESCON" on page 105 for a description of the IPv6 support added in z/OS V1R5 Communications Server for static XCF.

Restrictions

The following restrictions apply:

- The IP address specified on the IPCONFIG6 DYNAMICXCF parameter cannot be changed with a VARY TCPIP,,OBEYFILE command. You must first stop and then restart the TCP stack.

- IPCONFIG6 DYNAMICXCF does not support HiperSockets.
- A mix of static and dynamic IPv4 and IPv6 definitions for a device is not allowed. For example, if a static IUTSAMEH IPv4 device and link is defined, an IPv6 dynamic definition for IUTSAMEH will not be created. If a static IUTSAMEH IPv6 interface is defined, an IPv4 dynamic definition for IUTSAMEH will not be created. The same logic also applies for XCF links; a mix of static and dynamic IPv4 and IPv6 definitions is not allowed for an XCF link.

Coexistence requirements

To use IPv6 dynamic XCF links, all participating stacks must be at z/OS V1R5 Communications Server.

What this change affects

- Availability
- Customization
- Operations
- Performance

Using this function

If you want to use IPv6 support for dynamic XCF, perform the task in the following table.

Table 66. IPv6 support for dynamic XCF

Task	Procedure	Reference
Enable IPv6 dynamic XCF for each stack within the Sysplex.	On the IPCONFIG6 statement, code DYNAMICXCF specifying an IPv6 address.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

IPv6 support enhancements for Netstat

In z/OS V1R5 Communications Server, Netstat is changed in the following way for IPv6 support:

- The D TCPIP,,NETSTAT,ACCESS,NETWORK, Netstat CACHINFO/-C, IDS/-k, VCRT/-V, VDPT/-O, VIPADCFG/-F, VIPADYN/-v reports are enhanced to support LONG report format in preparation for future IPv6 support where applicable. The existing stack-wide output-format option (FORMAT SHORT/LONG) configured on the IPCONFIG profile statement, or Netstat FORMAT/-M option, can be used to instruct these Netstat reports to produce output according to either the old or new format.

See “Netstat enhancements” on page 74 for updates to Netstat in z/OS V1R5 Communications Server that are not related to IPv6 support. See “IPv6 support for Netstat” on page 153 for updates to Netstat in z/OS V1R4 Communications Server for IPv6 support. Refer to *z/OS Communications Server: IP System Administrator's Commands* for a complete description of the Netstat command.

Restrictions

None.

What this change affects

- Usability
- Diagnostics
- Operations

Using this function

If you want to use the Netstat command and its enhancements, perform the task in the following table.

Table 67. Netstat enhancements

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

IPv6 support enhancements for OMPROUTE

In z/OS V1R5 Communications Server, support for IPv6 dynamic routing is added to OMPROUTE. This includes support for IPv6 static routes, defined and learned IPv6 prefixes, and RIPng (RIP for IPv6).

Restrictions

The RIP limitation restricting multipath routes to directly connected interfaces has not been lifted.

Dependencies

IPv6 must be enabled in the TCP/IP stack.

What this change affects

- Availability
- Storage
- Operations
- Customization
- Performance

Using this function

If you want to use the IPv6 support enhancements for OMPROUTE, perform the tasks in the following table.

Table 68. IPv6 support enhancements for OMPROUTE

Task	Procedure	Reference
Enable IPv6 dynamic routing using IPv6 RIP.	Define IPv6 interfaces to OMPROUTE, using IPV6_RIP_INTERFACE statements for interfaces over which the IPv6 RIP protocol will be run, and using IPV6_INTERFACE statements for IPv6 interfaces over which no dynamic routing protocol will be run, if any.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Specify prefixes that reside on the link to which an interface attaches, which will not be advertised to this host by router discovery.	Define the Prefix parameter on the interface's IPV6_INTERFACE or IPV6_RIP_INTERFACE statements.	*z/OS Communications Server: IP Configuration Reference*
Define wildcard IPv6 interfaces.	Code IPV6_INTERFACE or IPV6_RIP_INTERFACE definition statements, using a wildcard interface name ending in *. For example VIPA* matches all interfaces whose names begin with the characters VIPA.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Define IPv6 default routes to the TCP/IP stack using OMPROUTE.	Code the IPV6_DEFAULT_ROUTE statement in the OMPROUTE configuration file.	*z/OS Communications Server: IP Configuration Reference*

Table 68. IPv6 support enhancements for OMPROUTE (continued)

Task	Procedure	Reference
Advertise this router as an IPv6 default router using IPv6 RIP.	Choose one of the following methods: • TCP/IP profile 1. Use BEGINROUTES in the TCP/IP profile to define static IPv6 default routes. 2. Enable advertisement of static routes into the IPv6 RIP autonomous system. • OMPROUTE configuration file 1. Code IPV6_ORIGINATE_RIP_DEFAULT statement.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Filter sending of IPv6 dynamic routes using IPv6 RIP.	Do one of the following: • Filter globally by coding one or more of the appropriate IPv6 sending filter statements: IPV6_RIP_FILTER (type nosend) IPV6_RIP_SEND_ONLY • Filter by interface by using the appropriate filter parameters on the IPV6_RIP_INTERFACE configuration statement.	*z/OS Communications Server: IP Configuration Reference*
Filter receipt of IPv6 dynamic routes using IPv6 RIP.	Do one of the following: • Filter globally by coding one or more of the appropriate IPv6 receiving filter statements: IPV6_RIP_FILTER (type noreceive) IPV6_IGNORE_RIP_NEIGHBOR • Filter by interface by using the appropriate filter parameters on the IPV6_RIP_INTERFACE configuration statement.	*z/OS Communications Server: IP Configuration Reference*
Force receipt of certain IPv6 RIP dynamic routes, regardless of other filters.	Code IPV6_ACCEPT_RIP_ROUTE statement.	*z/OS Communications Server: IP Configuration Reference*
Display OMPROUTE's IPv6 routing table.	Use the DISPLAY TCPIP,stackname,OMPROUTE,RT6TABLE command.	*z/OS Communications Server: IP System Administrator's Commands*
Display the full IPv6 RIP configuration on the host.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6RIP,ALL command.	*z/OS Communications Server: IP System Administrator's Commands*
Display IPv6 RIP information about local interfaces.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6RIP,INTERFACE command to see a summary of all IPv6 RIP interfaces. To see more detailed information about a specific IPv6 RIP interface, use the DISPLAY,TCPIP,stackname,OMPROUTE,IPV6RIP, INTERFACE,NAME=ifname command.	*z/OS Communications Server: IP System Administrator's Commands*
Display the list of IPv6 RIP global filters.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6RIP,FILTERS command.	*z/OS Communications Server: IP System Administrator's Commands*

Table 68. IPv6 support enhancements for OMPROUTE (continued)

Task	Procedure	Reference
Display the list of IPv6 RIP route updates that are to be unconditionally accepted by OMPROUTE.	Use the DISPLAY TCPIP,stackname,OMPROUTE,IPV6RIP,ACCEPTED command.	*z/OS Communications Server: IP System Administrator's Commands*
Set the MTU value for IPv6 interfaces.	Code the MTU value on the INTERFACE statement in TCP/IP profile. OMPROUTE will learn this value from TCP/IP. It is not necessary to code MTU values in OMPROUTE for IPv6 interfaces.	*z/OS Communications Server: IP Configuration Reference*
Use non-RIP IPv6 interfaces if all default values are acceptable.	No action needed. Unlike IPv4, it is not necessary to code all IPv6 interfaces to OMPROUTE if default values are acceptable.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Use non-RIP IPv6 interfaces if all default values are not acceptable.	Define the interface to OMPROUTE using the IPV6_INTERFACE statement.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Display IPv6 interfaces that are not running any routing protocol.	Use the DISPLAY TCPIP,tcpname,OMPROUTE,GENERIC6 commands.	*z/OS Communications Server: IP System Administrator's Commands*

IPv6 support for network access control

In z/OS V1R5 Communications Server, network access control is extended to IPv6 network addresses.

Restrictions

None.

What this change affects

- Application development
- Diagnosis
- Installation
- Operation
- Performance
- Security

Dependencies

Using network access control for IPv6 requires an IPv6 enabled stack (USS configuration required).

Using this function

If you want to use IPv6 support for network access control, perform the task in the following table.

Table 69. IPv6 support for network access control

Task	Procedure	Reference
Use network access IPv6 support.	Do the following: 1. Define fixed interface IDs for local interfaces by using an algorithm that makes link-local addresses unique across all local links 2. Define network security zones: • Identify groups of IP addresses that require the same access control policy. • Assign an eight character name to each group. 3. Define NETACCESS profiles: • Activate SERVAUTH CLASS. • Define NETACCESS profile for each network security zone. If access control policy is common across stacks, use generic profiles; otherwise, use specific profiles. • Authorize servers to profiles from which clients can communicate. • Authorize login users to profiles from which they may login. 4. Define NetAccess statement in TCPIP.PROFILE: • Map subnetworks and interface addresses to security zones. • Optionally, map unspecified local addresses with DEFAULTHOME. • Optionally, map unspecified addresses with DEFAULT.	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Security Server RACF Security Administrator's Guide*

Autoconfigure target library for FTP load module transfer

In z/OS V1R5 Communications Server, you can specify to FTP whether to create MVS directories as partitioned data sets (PDSs) or as partitioned data sets extended (PDSEs). Prior to this release, you could create an MVS PDS with FTP, but not a PDSE.

When transferring load modules, you must allocate an MVS directory on the target host before the transfer. The target MVS directory characteristics must be compatible with the source MVS directory for the transfer to succeed. Before this release, you had to determine the characteristics of the source directory and configure FTP with FTP.DATA statements, locsite subcommands, or SITE commands specifying the same characteristics before creating the directory. Now the mkdir and lmkdir subcommands do the configuration for you as they create the new directory. Specifically, in z/OS V1R5 Communications Server:

- The FTP client mkdir subcommand has a new *(like* parameter that allows you to create an MVS directory on the FTP server host with characteristics compatible with an MVS directory on the FTP client host.
- The FTP client lmkdir subcommand has a new *(like* parameter that allows you to create a local MVS directory with characteristics compatible with an MVS directory on the FTP server host.

Note: The FTP subcommands lmkdir and mkdir will change the local and remote site variables, respectively, if the new parameters are used.

Recommendations:

- FTP must open and read the source data set to calculate the DIRECTORY setting. Do not use the *(like* parameter if this is not acceptable.
- The *(like* parameter of the mkdir and lmdir subcommands is recommended for interactive use only.

Refer to *z/OS DFSMS: Using Data Sets* for more information about PDSs and PDSEs.

Restrictions

The following restrictions apply:

- The FTP client and server must both be z/OS V1R5 Communications Server or later.
- FTP can only approximate MVS directory characteristics such as SPACE, PRIMARY, and SECONDARY. For complete control over these characteristics, you should allocate MVS directories without the new subcommand parameters.
- Only the 3390 device architecture is supported. If the *(like* parameter is used with directories that reside on devices of other architectures, results are unpredictable.

What this change affects

- Customization
- Usability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Table 70. Autoconfigure target library for FTP load module transfer

Task	Procedure	Reference
Specify whether to allocate MVS directories in the client file system as partitioned data sets extended or partitioned data sets.	Code the PDSTYPE statement in the client's FTP.DATA.	*z/OS Communications Server: IP User's Guide and Commands*
For the current session only, specify whether to allocate MVS directories in the client file system as partitioned data sets extended or partitioned data sets.	Issue a locsite subcommand with the PDSTYPE parameter.	*z/OS Communications Server: IP User's Guide and Commands*
Specify whether to allocate MVS directories in the server file system as partitioned data sets extended or partitioned data sets.	Code the PDSTYPE statement in the server's FTP.DATA.	*z/OS Communications Server: IP Configuration Reference*
For the current session only, specify whether to allocate MVS directories in the server file system as partitioned data sets extended or partitioned data sets.	Issue a site subcommand with the PDSTYPE parameter.	*z/OS Communications Server: IP User's Guide and Commands*
Allocate an MVS directory in the client's file system similar to a directory in the server's file system.	Issue a lmkdir subcommand with the *(like* parameter.	*z/OS Communications Server: IP User's Guide and Commands*
Allocate an MVS directory in the server's file system similar to a directory in the client's file system.	Issue a mkdir subcommand with the *(like* parameter.	*z/OS Communications Server: IP User's Guide and Commands*

Define FTP ephemeral port range for firewall compatibility

In z/OS V1R5 Communications Server, FTP sessions through firewalls are enhanced in two ways:

- You can configure the FTP server to select ephemeral ports from a specific range of values compatible with your firewall configuration.
- IPv4 security-protected and encrypted sessions through Network Address Translation (NAT) firewalls are enabled.

These enhancements are beneficial for the following reasons:

- When an FTP control connection using IPv4 protocol is encrypted, as it will be if you are using SSL/TLS security or Kerberos, the session cannot traverse Network Address Translation (NAT) firewalls. This is because NAT firewalls monitor the control connection for PORT and PASV commands, changing the IP addresses in PORT commands and PASV replies. If the control connection is encrypted, the NAT firewall cannot monitor it.

  RFC 2428 describes an alternative to the PORT and PASV commands for establishing a data connection: the EPSV command. The key fact about the EPSV command is that neither the command nor its reply includes an IP address, so establishing a data connection through an NAT firewall is not a problem. z/OS V1R4 Communications Server FTP implemented RFC 2428, but only on IPv6 FTP sessions.

  This z/OS V1R5 Communications Server enhancement adds a configuration option to direct the FTP client to use the EPSV command instead of PORT or PASV commands to establish the data connection for an IPv4 FTP session.
- FTP allows the operating system to select port numbers used for listening data sockets. Some firewall implementations can be configured to restrict the range of port numbers allowed to applications such as FTP. This enhancement allows you to configure the FTP server to select listening data ports from a specific range of values so you can coordinate the FTP server with your firewall configuration. You can configure this range with the PASSIVEDATAPORTS statement in FTP.DATA. In conjunction with PASSIVEDATAPORTS, IBM suggests reserving the range of ports with the new PORTRANGE AUTHPORT statement in PROFILE.TCPIP.

Restrictions

The following restrictions apply:

- If the FTP server rejects either the EPSV or EPRT command during the FTP session, the client will stop sending EPSV to the server regardless of whether you have specified use of EPSV on IPv4 sessions.
- Socksified sessions use PASV or PORT to establish data connections depending on the FWFRIENDLY setting. When EPSV4 is set, the client will try EPSV but never EPRT to establish a socksified data connection.

Incompatibilities

Some servers support the EPSV command, but do not reply in the format described in RFC 2428. The z/OS FTP client does not support such servers. If the FTP server reply to EPSV does not conform to RFC 2428, the client will react as if the server had rejected the EPSV command, and will stop using EPSV during the session.

Dependencies

The FTP server must support the EPSV command for IPv4 sessions. The z/OS FTP server supports RFC 2428 (that is, EPSV and EPRT commands) for both IPv4 and IPv6 sessions.

What this change affects

- Customization
- Installation
- Security
- Usability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Table 71. Define FTP ephemeral port range for firewall compatibility

Task	Procedure	Reference
Enable EPSV command usage for all FTP IPv4 sessions.	Code EPSV4 TRUE in the client's FTP.DATA.	*z/OS Communications Server: IP User's Guide and Commands*
Override EPSV4 setting in FTP.DATA for a specific session.	Issue a locsite subcommand with the EPSV4 or NOEPSV4 parameter.	*z/OS Communications Server: IP User's Guide and Commands*
Restrict server's listening data socket port numbers to a specific range of values.	Do the following: • Add a PASSIVEDATAPORTS statement to server's FTP.DATA. • Add one or more PORTRANGE AUTHPORT statements to PROFILE.TCPIP for the same range of ports as specified on the PASSIVEDATAPORTS statement.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Restrict the port number that the server sends to the client in an EPSV or PASV reply to a certain range of values.	Do the following: • Add a PASSIVEDATAPORTS statement to server's FTP.DATA. • Add one or more PORTRANGE AUTHPORT statements to PROFILE.TCPIP for the same range of ports as specified on the PASSIVEDATAPORTS statement.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

FTP TLS support enhancements

In z/OS V1R5 Communications Server, the FTP server can be configured to allow a user to log in without specifying a password. The server will use the TLS authenticated X.590 certificate provided by the FTP client to perform this login. This support allows you to take advantage of using a certificate instead of a password to complete the login procedure.

Restrictions

None.

Dependencies

This support is for an FTP session that meets the following conditions:

- The session is protected by the TLS security mechanism.
- The client sends a certificate to the server during the TLS handshake procedure. The certificate is required if SECURE_LOGIN VERIFY_USER or SECURE_LOGIN REQUIRED is coded in the FTP.DATA file of the server.
- The certificate is registered in the security product.
- The name associated with the certificate in the security product is the same name that is on the USER command.

What this change affects

- Security
- Usability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Table 72. Enhance FTP TLS support

Task	Procedure	Reference
Create a TLS environment that provides a client certificate.	See "Dependencies" for the information necessary for this task.	*z/OS Communications Server: IP Configuration Reference*
Enable a client to log in without requiring a password.	In FTP.DATA for the server, code SECURE_PASSWORD OPTIONAL.	*z/OS Communications Server: IP Configuration Reference*

Improve FTP serviceability

z/OS V1R5 Communications Server enhances diagnosis of failures in the FTP server and client. The enhancements include the following areas:

- Client error logging to the system log is provided (see "Enforce nonzero error return code in FTP" on page 117).
- Client error codes are extended to further describe failures in the client (see "Enforce nonzero error return code in FTP" on page 117).
- Dynamic allocation failure reporting is enhanced to ensure all failures record needed information. This includes S99ERROR, S99INFO, and S99ERSN.
- All Language Environment® (LE) and UNIX System Services (USS) failure reporting, including errnojr (referred to as errno2), is provided.
- Message EZA2589E text is changed to include the failing operation.

Restrictions

None.

What this change affects

- Diagnostics

Using this function

This enhancement does not require any action to take advantage of the new function. Review the following table for information about changes in the interface.

Table 73. Improve FTP serviceability

Task	Procedure	Reference
Receive SVC 99 failure information.	No action is required. Some replies do not report S99ERSN. If the failure occurs in the server and you believe the S99ERSN field is of interest, you can obtain it from the trace or FTPLOGGING data on the server. Message EZA2562W is corrected to always display all failure data available.	*z/OS Communications Server: IP User's Guide and Commands* and *z/OS Communications Server: IP Messages Volume 1 (EZA)*
Receive complete description of Language Environment and UNIX System Services failures.	No action is required. Existing trace entries and messages are updated to include the full description of the error. The messages that will now include the errnojr information (referred to as errno2) in their output are: • EZA2580E • EZA2668W • EZA2669W • EZY2693I • EZA2863I • EZA2864I • EZYFT01I • EZYFT08W • EZYFT40E • EZYFT48E • EZYFS69I • EZYFT33I • EZYFT15E • EZYFT16E • EZYFT53E • EZYFT12E • EZYFT13E • EZYFT14E • EZYFT17E • EZYFS79I • EZY2673E • EZY2691E Replies that currently display Language Environment/UNIX System Services error messages will now include the errno2 data as well.	*z/OS Communications Server: IP User's Guide and Commands*, *z/OS Communications Server: IP Messages Volume 1 (EZA)*, and *z/OS Communications Server: IP Messages Volume 3 (EZY)*
Be aware that the content of the messages listed for Language Environment and UNIX System Services failures has changed slightly.	No action is required. Where the error description is included, there will be additional text describing the errnojr field. The errnojr setting will normally be zeroes if it is not significant for the called function. Note that errnojr is referred to as errno2. Example: EDC5121I Invalid argument. (errno2=0x0C0F8402)	*z/OS Language Environment Run-Time Messages* and *z/OS UNIX System Services Messages and Codes*

Table 73. Improve FTP serviceability (continued)

Task	Procedure	Reference
Receive location of failure when message EZA2589E is issued.	No action is required. The text of the message now includes an operation field which describes where the failure was detected and *z/OS Communications Server: IP Diagnosis Guide* contains a new section on diagnosing the failures reported in EZA2589E.	*z/OS Communications Server: IP Messages Volume 1 (EZA)* and *z/OS Communications Server: IP Diagnosis Guide*
Be aware of changes to message EZYFT71.	Message EZYFT71I has been changed to EZYFT71E and the format of the message has changed slightly. This message is used to report certain terminating errors encountered in the server or daemon.	*z/OS Communications Server: IP Messages Volume 3 (EZY)*

Enforce nonzero error return code in FTP

In z/OS V1R5 Communications Server, the new LOGCLIENTERR and updated CLIENTERRCODES statements direct the FTP client to provide enhanced diagnostic information when the client detects a failure. Specifically:

- LOGCLIENTERR will generate a message on the system log and the batch job log (or return it to the user in an interactive environment) with complete information about the command code, reply code, and computed return code related to the failure.
- CLIENTERRCODES has a new option, EXTENDED, to append the code of the failing subcommand to the client error code for the batch or interactive return code. Several client error codes are new in z/OS V1R5 Communications Server and all the possible client error codes are set more consistently and reliably.

In addition, the text for message EZA1735I has changed from:

```
EZA1735I FTP Return Code = rc, Error Code = ec
```

to

```
EZA1735I Std Return Code = rc, Error Code = ec
```

This change more accurately reflects the contents of the message since the actual return code in the FTP client may not be a standard return code.

Restrictions

None.

What this change affects

- Customization
- Diagnostics

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Table 74. Enforce nonzero error return code in FTP

Task	Procedure	Reference
Enable logging of failures reported by the FTP client.	Add LOGCLIENTERR TRUE to the FTP.DATA file for the client.	*z/OS Communications Server: IP User's Guide and Commands*
Interpret logged information for FTP client failures.	Look up message EZZ9830I and the contents returned in it.	*z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)* and *z/OS Communications Server: IP User's Guide and Commands*
Request new FTP client return codes based on the CLIENTERRCODES and subcommand codes.	Specify CLIENTERRCODES EXTENDED in the FTP.DATA file for the client.	*z/OS Communications Server: IP User's Guide and Commands*
Interpret new FTP client return codes based on the CLIENTERRCODES and subcommand codes.	Look up client error codes and subcommand codes.	*z/OS Communications Server: IP User's Guide and Commands*
Receive more consistent and reliable information in client error codes.	No action is required. The client error codes have been expanded and are set more often and more reliably in the FTP client for original client error codes and EXTENDED client error codes.	*z/OS Communications Server: IP User's Guide and Commands*
Receive batch job return codes in decimal format using the DIR command under FILETYPE=JES.	No action is required. The DIR display under FILETYPE=JES has been changed to display batch job return codes in decimal format.	*z/OS Communications Server: IP User's Guide and Commands*

Allow the FTP server load module to run above the 16M line

In z/OS V1R5 Communications Server, the FTP server load module EZAFTPLS (alias ftpdns) is linkedited with RMODE=ANY so that it can be loaded above the 16M line. This is an enhancement because below the line space is a limited resource.

Restrictions

None.

What this change affects

- Storage

Using this function

This enhancement will not require any action to implement; in z/OS V1R5 Communications Server when FTP is installed, the linkedit occurs with RMODE=ANY. However, if you have previously coded your security exits to have the dependency of working below the line, you should examine the exits and modify them appropriately.

Display status of FTPKEEPALIVE timer

Prior to z/OS V1R5 Communications Server, the FTP client LOCSTAT subcommand displayed all client timers except the FTPKEEPALIVE timer. In z/OS V1R5 Communications Server, the following enhancements were made:

- LOCSTAT was enhanced to also display the FTPKEEPALIVE timer.
- The FTP STAT subcommand displays the value of the server's FTPKEEPALIVE timer.

Restrictions

None.

Dependencies

The SUPPRESSIGNOREWARNINGS statement is effective only for statements that follow it in FTP.DATA.

What this change affects

- Customization
- Usability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Table 75. Display status of FTPKEEPALIVE timer

Task	Procedure	Reference
Display the value of the FTP client's FTPKEEPALIVE timer.	Issue a LOCSTAT subcommand.	*z/OS Communications Server: IP User's Guide and Commands*
Set the client's FTPKEEPALIVE timer.	Add an FTPKEEPALIVE statement to the client's FTP.DATA.	*z/OS Communications Server: IP User's Guide and Commands* and *z/OS Communications Server: IP Configuration Reference*
Display the value of the FTP server's FTPKEEPALIVE timer.	Issue a STAT subcommand to the server.	*z/OS Communications Server: IP User's Guide and Commands*
Set the server's FTPKEEPALIVE timer.	Add an FTPKEEPALIVE statement to the client's FTP.DATA.	*z/OS Communications Server: IP User's Guide and Commands* and *z/OS Communications Server: IP Configuration Reference*
Suppress messages EZYFT47I issued by the client when reading FTP.DATA.	Add a SUPPRESSIGNOREWARNINGS statement to the client's FTP.DATA.	*z/OS Communications Server: IP User's Guide and Commands* and *z/OS Communications Server: IP Configuration Reference*
Suppress messages EZYFT47I logged by the server when reading FTP.DATA	Add a SUPPRESSIGNOREWARNINGS statement to the server's FTP.DATA.	*z/OS Communications Server: IP Configuration Reference*

FTP SERVAUTH Port of Entry support

The FTP daemon uses NETACCESS profiles in the SERVAUTH class for Port of Entry authorization for IPv6 clients. The FTP daemon may optionally be migrated to use NETACCESS profiles instead of profiles in the TERMINAL class for Port of Entry authorization for IPv4 clients.

Note: Programs invoked by the z/OS INET daemon that perform login or change identity will also use NETACCESS profiles in the SERVAUTH class for Port of Entry authorization when the client's IP address is mapped in a NETACCESS zone.

Restrictions

None.

Dependencies

The FTP Port of Entry authorization support, using NETACCESS SERVAUTH profiles, requires a NETACCESS statement configured in the TCPIP PROFILE and security server support for the SERVAUTH= parameter on SAF macro RACROUTE REQUEST=VERIFY. The NETACCESS statement includes support for IPv6. RACF, in z/OS V1R5, provides support for the SERVAUTH parameter on the RACROUTE REQUEST=VERIFY macro.

What this change affects

- Customization
- Security
- Usability

Using this function

If you want to use the FTP SERVAUTH Port of Entry support, perform the task in the following table.

Table 76. FTP SERVAUTH Port of Entry support

Task	Procedure	Reference
Enable FTP SERVAUTH Port of Entry support.	Do the following: • Define network security zones: – Activate SERVAUTH CLASS. – Define NETACCESS profile for each network security zone. – Authorize FTPD to NETACCESS profiles from which any client may login. – Authorize FTP login users to NETACCESS profiles from which they may login. • Decide if FTP Daemon should use SERVAUTH for only IPv6 clients or for both IPv4 and IPv6 clients. • Optionally migrate IPv4 clients to SERVAUTH by adding a PORTOFENTRY4 SERVAUTH statement to FTP.DATA. • Define datasets to have limited access by Port of Entry – Add/Modify profiles in DATASET CLASS – Permit users to dataset profiles WHEN(SERVAUTH(...))	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Security Server RACF Security Administrator's Guide*

TN3270 IP address range configuration

In z/OS V1R5 Communications Server, IP ranges can be specified in IPGROUP or DESTIPGROUP statements in addition to exact IP addresses and IP subnets.

Restrictions

Only the right-most portion of the IP address can be part of the range. For IPv4 addresses, that is the last octet, and for IPv6 addresses that is the last two hexadecimal bytes.

What this change affects

- Customization

Using this function

If you want to take advantage of TN3270 IP address range configuration, perform the task in the following table.

Table 77. TN3270 IP address range configuration

Task	Procedure	Reference
Specify an IP range for the TN3270 parm, IPGROUP and DESTIPGROUP.	Use the new double dotted notation to specify the first and last IP address in the range.	*z/OS Communications Server: IP Configuration Reference*

TN3270 Takeover enhancement

In z/OS V1R5 Communications Server, Telnet supports takeover of connections without the end user having to specify an LU name.

When a connection is lost but still considered active by Telnet, the LU cannot be reused and the application session remains. The end user cannot reconnect to that session until an inactivity timer causes the session to drop. TKOSPECLU solves this problem for end users who specify an LU name at connection request time. Most end users do not specify an LU name and are not able to take advantage of the takeover function. With TKOGENLU and TKOGENLURECON, a single connection can be taken over by an end user from the same client.

Restrictions

Only one connection can be taken over. Clients with multiple connections will see a delay in connection requests after the first connection.

What this change affects

- Customization
- Availability

Using this function

If you want to take advantage of the TN3270 Takeover enhancement, perform the task in the following table.

Table 78. TN3270 Takeover enhancement

Task	Procedure	Reference
Enable takeover using KeepLU function.	Specify TKOGENLU and TKOGENLURECON in one of the three Telnet parameter blocks, TelnetGlobals, TelnetParms, or ParmsGroup.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

TN3270 keyboard control enhancements

In z/OS V1R5 Communications Server, the Telnet Server allows customized control of the keyboard unlock function in conjunction with SNA read commands received from the host application. This control is implemented by a new TCP/IP profile parameter called UNLOCKKEYBOARD. Use of this parameter enables the system programmer to dictate whether a 3270 unlock keyboard datastream sequence is sent to a TN3270 client before or after a read command is forwarded from the host application.

UNLOCKKEYBOARD also provides control over whether or not a clear screen and unlock keyboard sequence are sent to TN3270 clients when Telnet receives the application BIND.

In addition, the Telnet Server will more fully implement the TN3270E functional extensions to RFC 2355 by employing use of the Keyboard Restore Indicator (KRI) in the TN3270E header. There are no external changes associated with this functional extension to RFC 2355.

Restrictions

None.

What this change affects

- Customization

Using this function

If you want to use the new customized control of the keyboard, perform the task in the following table.

Table 79. TN3270 Keyboard control enhancements

Task	Procedure	Reference
Enable a host application that sends 3270 Read Configuration commands to work with a client using a typahead feature.	Specify the UNLOCKKEYBOARD parameter with the appropriate parameters.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

IPv6 support for TN3270

In z/OS V1R5 Communications Server, the Telnet Server supports IPv6 format IP addresses, depending on the support level of the TCP/IP stack. If the stack is running IPv6, Telnet completely supports IPv6. If the stack is running IPv4, Telnet is IPv4 capable. There is no external parameter needed in Telnet to turn on IPv6 support. Telnet is always IPv6 capable if the stack supports IPv6. If the TCP/IP stack is running in IPv4 mode, no IPv6 function is available in Telnet.

Displays that are tabular in style will use a two-line format to display the data when a client identifier appears on the line if either of the following IPv6 switch conditions are met:

- The stack is running IPv6 mode.
- The configuration statement FORMAT LONG is specified.

If the new two-line format is used, it is always used even when the data would fit on a single line. This will ensure uniformity of output for displays.

Restrictions

The WLM statement does not support the IPv6 format.

Dependencies

The TCP/IP stack must be IPv6 enabled.

What this change affects

- Customization

Using this function

If you want to take advantage of the IPv6 support for TN3270, perform the task in the following table.

Table 80. IPv6 support for TN3270

Task	Procedure	Reference
Enable IPv6 addresses.	Code IPv6 addresses as needed in the Telnet profile statement blocks.	*z/OS Communications Server: IP Configuration Reference*

TN3270 Network Management

In z/OS V1R5 Communications Server, monitoring of the total Telnet transaction can be done within the Telnet Server. Monitoring is requested by using the new TN3270 Server Profile statements, MONITORGROUP and MONITORMAP. The transaction data can then be retrieved by using either the D TCPIP,,TELNET,CONN,CONN=connid detail command or by using SNMP. The SNMP support is provided by a new SNMP TN3270 Telnet subagent. The SNMP transaction data is defined in a new Enterprise-specific TN3270 MIB. A sample of this MIB is installed in the HFS as file /usr/lpp/tcpip/samples/mvstn3270.mi2. Activation of the SNMP TN3270 Telnet subagent is controlled by the new TNSACONFIG Profile statement. Refer to *z/OS Communications Server: IP Configuration Reference* for more detailed information on all the new TN3270 Telnet Server Profile statements.

Note: Requests from the management application may cause a reduction in performance.

For a description of the transaction data provided by the TELNET detail command, refer to message EZZ6065I in *z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)*. For a description of the SNMP MIB data, refer to the SNMP topic of *z/OS Communications Server: IP System Administrator's Commands*.

Restrictions

None.

Dependencies

The SNMP Telnet transaction data will only be available on TCP/IP stacks where the TN3270 Telnet server is active and where there are Telnet connections being monitored for transaction data due to MONITORGROUP and MONITORMAP Profile statements.

What this change affects

- Diagnosis
- Performance

Using this function

If you want to take advantage of TN3270 Network Management function, perform the tasks in the following table.

Table 81. TN3270 Network Management

Task	Procedure	Reference
Start the Telnet subagent.	Specify the TNSACONFIG statement.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Define monitoring parameters.	Specify a MONITORGROUP statement.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Map the monitoring parameters to clients	Specify a MONITORMAP statement that maps the group to a Client Identifier.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Retrieve monitored transaction data.	Invoke the D TCPIP,,TELNET,CONN,CONN=connid command or retrieve the data from SNMP.	*z/OS Communications Server: IP System Administrator's Commands*
Display the MonitorGroup Object.	Invoke the D TCPIP,,TELNET,OBJECT,TYPE=mongrp command.	*z/OS Communications Server: IP System Administrator's Commands*

Improve performance for TN3270 definite response sessions

In z/OS V1R5 Communications Server, the TN3270E server can turn off DELAYACKS for TN3270E clients that have negotiated a definite response.

Restrictions

None.

What this change affects

- Performance

Using this function

There are no exploitation procedures associated with this enhancement.

Network Access Control for TN3270

Administrators can now restrict the access of TN3270 ports using security zones. With this support, the TN3270 server can now participate in Network Access Control and the granularity of security access that it provides.

Restrictions

Use of NACUSERID in TELNETGLOBALS block of PROFILE.TCPIP assumes that Network Access Control is being used on all TN3270 ports that do not already have a NACUSERID defined in that port's TELNETPARMS block. A NONACUSERID may be used in a TELNETPARMS block to cancel the effects of the NACUSERID defined in TELNETGLOBALS for that TN3270 port.

Dependencies

None.

What this change affects

- Security
- Customization

Using this function

If you want to use Network Access Control for TN3270, perform the task in the following table.

Table 82. Network Access Control for TN3270

Task	Procedure	Reference
Establish Network Access Control for TN3270.	Perform the following steps: 1. Define local and remote network Security Zones using the NETACCESS statement in PROFILE.TCPIP. 2. Define NETACCESS profiles in SAF SERVAUTH class and activate SERVAUTH class. 3. Define TN3270 ports using PORT statement in PROFILE.TCPIP. 4. Define TN3270 NACUSERID for TN3270 ports in the TELNETGLOBALS and/or TELNETPARMS blocks of PROFILE.TCPIP. 5. If TN3270 bind IP address (INADDRANY or specific override in PORT statement) is in a Security Zone, permit NACUSERID to corresponding NETACCESS profile. 6. For each Security Zone that contains clients that you want to allow to use that TN3270 port, permit NACUSERID to corresponding NETACCESS profile. 7. Activate Network Access Control by specifying NetAccess INBOUND OUTBOUND in PROFILE.TCPIP.	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Security Server RACF Security Administrator's Guide*

Multilevel security LU name assignment support for TN3270

In a multilevel security environment, security label checking will further ensure data is not declassified through the TN3270 leg of the connection. Also, TN3270 ensures that the SECLABEL of the TCP/IP connection and the TN3270 LU name are equivalent, enabling end-to-end control. This allows SNA applications that engage in multilevel security checking to use the Security Label of the LU name as if it were the Security Label of the TCP/IP connection.

Restrictions

None.

Dependencies

None.

What this change affects

- Security

Using this function

If you want to use multilevel security LU name assignment support for TN3270, perform the task in the following table.

Table 83. Multilevel security LU name assignment support for TN3270

Task	Procedure	Reference
Establish multilevel security LU name assignment support.	Perform the following steps: 1. Define Security Labels in SAF SECLABEL class and activate SECLABEL class. 2. Define local and remote network Security Zones using NETACCESS statement in PROFILE.TCPIP. 3. Define NETACCESS profiles with SECLABEL in SAF SERVAUTH class and activate SERVAUTH class. 4. Define LU Names with SECLABEL in SAF TERMINAL class and activate TERMINAL class. 5. Define LU Names with equivalent SECLABEL into TN3270 LU Groups in PROFILE.TCPIP. 6. Ensure configured NACUSERID has appropriate Security Label (may be SYSMULTI if stack user ID is SYSMULTI).	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Planning for Multilevel Security and the Common Criteria*

SNMP agent

The SNMP agent is enhanced to allow IPv6 support for SNMP applications.

IPv6 support for SNMP applications

The SNMP agent, osnmp command, Trap Forwarder daemon and Distributed Protocol Interface for SNMP subagents are all enhanced to operate over IPv6 networks and handle IPv6-related management data. The pwtokey and pwchange commands are enhanced to accept IPv6 addresses as input.

API change

The Distributed Protocol Interface (DPI®) version 2.0 is enhanced with the ability to use IPv6 connectivity if available. This affects the routines DPIconnect_to_agent_TCP() and DPIconnect_to_agent_UNIXstream().

Restrictions

When the SNMP agent is started, it retrieves a local host IP address for itself. If this is an IPv6 address, then SNMPv1 traps will be sent with 0.0.0.0 encoded as the source address. This can be prevented by using the -A option on the osnmpd command to force the agent to get an IPv4 address when it initializes. Refer to *z/OS Communications Server: IP Configuration Reference* for details.

Dependencies

To take advantage of the IPv6 support offered by the SNMP agent, the osnmp command, and trap forwarder daemon, the TCP/IP stack must be IPv6 enabled. If not, these applications will operate in IPv4 mode.

Incompatibilities

The algorithm used for generating the engineID for SNMPv3 authentication and privacy has been changed to support a more current standard. Existing key definitions will continue to work as long as the SNMP agent engineID is not changed. If the SNMP agent engineID is changed (for example, by removing the SNMPD.BOOTS file and letting the agent regenerate its engineID), localized keys must be regenerated using the new engineID format.

What this change affects

- Customization
- Operations
- Application development
- Diagnosis
- Availability

Using this function

If you want to use the IPv6 support for SNMP applications, perform the tasks in the following table.

Table 84. IPv6 support for SNMP applications

Task	Procedure	Reference
Configure the SNMP agent to use IPv6 connectivity.	Update SNMPD.CONF or update PW.SRC and SNMPTRAP.DEST to use IPv6 addresses.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Configure osnmp to use IPv6 connectivity.	Update OSNMP.CONF to use IPv6 targetAgent addresses.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Enable Trap Forwarder daemon to use IPv6 connectivity.	Update TRAPFWD.CONF to use IPv6 host_name addresses.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Optionally, make configuration updates to use new SNMPv3 engineID format.	Remove the SNMPD.BOOTS file so the SNMP agent will regenerate its engineID upon restart. Use pwtokey to regenerate any localized SNMPv3 keys used by the SNMP agent (SNMPD.CONF) and any SNMPv3 network managers, such as osnmp (OSNMP.CONF), with the new engineID.	*z/OS Communications Server: IP Configuration Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Communications Server: IP System Administrator's Commands*

SNMP TCP/IP subagent

z/OS V1R5 Communications Server includes the following enhancements for the SNMP TCP/IP subagent:

- Support for IPv6 MIB data. The IPv6 MIB data is supported in version-neutral MIB objects. Version-neutral MIB objects can support both IPv4 and IPv6 processing. The TCP/IP subagent now supports some version-neutral standard MIB data from the following Internet drafts:
  - IP-MIB from draft-ietf-ipv6-rfc2011-update-01.txt
  - TCP-MIB from draft-ietf-ipv6-rfc2012-update-01.txt
  - IP-FORWARD-MIB from draft-ietf-ipv6-rfc2096-update-02.txt

Copies of these versions of the Internet drafts are shipped with z/OS V1R5 Communications Server and installed in the HFS in the /usr/lpp/tcpip/samples directory with the following file names:
  - ipfwdmib.mi2 - IP-FORWARD-MIB
  - ipmib.mi2 - IP-MIB
  - tcpmib.mi2 - TCP-MIB

  Even though the IPv4-only MIB data in these Internet drafts has been deprecated, the TCP/IP subagent continues to support this data. The ifTable, ifXTable, and ifStackTable from RFC 2233 will now contain IPv6 interface information. The IBM MVS TCP/IP Enterprise-specific MIB has been enhanced for IPv6 support as follows:
  - The ibmTcpipMvsTcpListenerTable will now support IPv6 servers
  - New MIB objects, ibmMvsPortBindIpAddressType and ibmMvsPortBindIpAddress, have been added to the ibmTcpipMvsPortTable. These MIB objects support either an IPv4 or IPv6 IP address specified on the BIND keyword of the PORT Profile statement.
- New ibmTcpipMvsPktTraceTable in the IBM MVS TCP/IP Enterprise-specific MIB. Each entry represents a unique set of packet trace parameters per interface.
- New MVS system name and sysplex name MIB objects in the IBM MVS TCP/IP Enterprise-specific MIB.
- New SACACHETIME parameter on the SACONFIG Profile statement. This parameter permits the TCP/IP subagent cache time to be changed using the subagent's Profile statement. Previously, the only way to change this cache time was by using an snmp set request for MIB object ibmMvsSubagentCacheTime.
- A new error message, EZZ3231I, will be issued to the console when the Subagent can not obtain storage to process SNMP requests. The message will be issued once every 15 minutes while the low storage condition exists.
- New or changed Dynamic VIPA MIB data in the IBM MVS TCP/IP Enterprise-specific MIB.
  - New ibmMvsDVIPADistPortDynamicFlag MIB object added to the existing ibmMvsDVIPADistPortTable.
  - New ibmMvsDVIPADistConfTimedAffinity MIB object added to the existing ibmMvsDVIPADistConfTable.
  - Changed the description of the ibmMvsDVIPADistConfPort object
- New interface data in the IBM MVS TCP/IP Enterprise-specific MIB.

  The following new MIB objects were added to the ibmTcpipMvsLinkTable:
  - ibmMvsLinkVlanId
  - ibmMvsLinkVlanPriorityEnabled
  - ibmMvsLinkReadStorageSize
  - ibmMvsLinkInboundPerfType
  - ibmMvsLinkChecksumOffloadEnabled
- New TCP connection data in the IBM MVS TCP/IP Enterprise-specific MIB.
  - New ibmMvsTcpListenerCurrConns MIB object added to the existing ibmTcpipMvsTcpListenerTable.
- The following MIB objects in the IBM MVS TCP/IP Enterprise-specific MIB were deprecated:
  - ibmMvsPortOptMaxSegmentSize - the TCP/IP stack no longer supports the OPTMSS parameter on the PORT Profile statement.
  - ibmMvsTcpConnOptMaxSegmentSize - the TCP/IP stack no longer supports the SO_OPTMSS socket option and the OPTMSS parameter on the PORT Profile statement.

  - ibmMvsPortBindIpAddr - This object was replaced by new objects, ibmMvsPortBindIpAddressType and ibmMvsPortBindIpAddress
  - ibmTcpipMvsGatewayTable - This table augments the standard ipForwardTable, which was deprecated.
  - ibmTcpipMvsTcpConnTable - This table augments the standard tcpConnTable which was deprecated
- The ifAdminStatus MIB object from the IF-MIB (RFC 2233) will now reflect the desired state of an interface. If a START command has been invoked for an interface, ifAdminStatus will be set to up(1). If an interface has never been started or, if a STOP command has been invoked for an interface, ifAdminStatus will be set to down(2).

Refer to the TCP/IP Subagent topic of the SNMP chapter in *z/OS Communications Server: IP System Administrator's Commands* for a detailed description of the supported MIB data.

What this change affects

- Customization
- Operations
- Usability

Dependencies

In order to retrieve SNMP IPv6 data, the TCP/IP stack associated with the subagent must be enabled for IPv6 support.

Using this function

If you want to use the IPv6 support and enhancements for the SNMP TCP/IP subagent, perform the task in the following table.

Table 85. IPv6 support and enhancements for the SNMP TCP/IP subagent

Task	Procedure	Reference
Use the new or changed MIB objects from network management applications or from the z/OS UNIX snmp command.	The action to take depends on the management application. For the snmp command, no action is required. For the NetView SNMP command, use the most current copy of the sample MIBDESC.DATA file, which is shipped in SEZAINST(MIBDESC). Other management applications may require different changes.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

SNMP Network SLAPM2 subagent

z/OS V1R5 Communications Server introduces a new SNMP Network SLAPM2 subagent replaces the old SLA subagent. The new SNMP Network SLAPM2 subagent application (nslapm2) contains the information that can be used to analyze network performance for respective policy.

Restrictions

The new SNMP Network SLAPM2 subagent does not regulate traffic that is not originated in the host with the service level policies (such as routed traffic).

Incompatibilities

The SLAPM-MIB Object IDs (OIDs) for the MIB objects supported by the SLA subagent (pagtsnmp) will not work with the new Network SLAPM2 subagent (nslapm2). In order to avoid this problem, either start the SLA subagent to execute the old SLAPM-MIB, or start the Network SLAPM2 subagent to execute the new NETWORK-SLAPM2-MIB.

Dependencies

The following TCP/IP applications must be active:

- Policy Agent (Pagent) with the PolicyPerformanceCollection statement in Policy Agent configuration file enabled for the TCP/IP stack for which the Network SLAPM2 subagent is configured.
- SNMP Agent

What this change affects

- Performance.

Using this function

If you want to use the SNMP Network SLAPM2 subagent, perform the tasks in the following table.

Table 86. SNMP Network SLAPM2 subagent

Task	Procedure	Reference
Enable policy performance data collection.	Specify the PolicyPerformanceCollection statement in the Policy Agent configuration file for each stack for which Network SLAPM2 subagent will be activated.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Start new Network SLAPM2 subagent (nslapm2).	Do the following: 1. Start Policy Agent. 2. Start SNMP Agent. 3. Start the new subagent from the shell /bin/nslapm2 or a started procedure from SEZAINST. IBM recommends that this new subagent executes in place of the SLA subagent (pagtsnmp).	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*
Use the new NETWORK-SLAPM2- MIB objects.	The new NETWORK-SLAPM2-MIB is shipped in /usr/lpp/tcpip/samples in file slapm2.mi2.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*

SNMP TN3270 Telnet subagent

z/OS V1R5 Communications Server provides a new SNMP TN3270 Telnet subagent. This subagent provides Telnet transaction data for monitored Telnet connections by using the SNMP protocol. See "TN3270 Network Management" on page 123 for more introductory information on this subagent.

z/OS UNIX osnmp/snmp command enhancement

A usability enhancement was made in the way the osnmp command displays MIB objects of type Counter64. They will now be displayed as decimal equivalents of the 64-bit field.

New SNMP MIB modules

z/OS Communications Server ships several Enterprise-specific MIB modules that are installed in the /usr/lpp/tcpip/samples HFS directory. Refer to the SNMP topic of *z/OS Communications Server: IP System Administrator's Commands* for a complete listing of all the enterprise-specific MIB modules shipped with z/OS Communications Server. Currently, both an SMIv1 and SMIv2 version is shipped for some of the MIB modules. Support for providing the SMIv1 version of these MIB modules will be dropped in a future release. For the Enterprise-specific MIB modules that are new for z/OS V1R5 Communications Server, only an SMIv2 version is provided. You can use tools such as libsmi to create the SMIv1 equivalent of a MIB module defined in SMIv2.

The following Enterprise-specific MIB modules are new for z/OS V1R5 Communications Server:

Table 87. Enterprise-specific MIB modules that are new for z/OS V1R5 Communications Server

Function	Enterprise-specific MIB module
TN3270 Telnet subagent	mvstn3270.mi2
Network SLAPM2 subagent	slapm2.mi2

Chapter 5. V1R4 IP new function summary

This chapter includes a section for every function or enhancement introduced for IP in z/OS V1R4 Communications Server. The sections include the following 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. The tables include references to the documents that contain more detailed information for each task.

See Table 8 on page 25 for a complete list of the IP functional enhancements of the current and recent releases.

Refer to *z/OS Migration* for information about how to maintain the functional behavior of previous releases. Refer to *z/OS Summary of Message and Interface Changes* for information on new and changed messages and interfaces.

General considerations

In addition to the function-specific tasks of this chapter, be aware of the following general considerations:

- This release introduces support for IPv6 addressing for certain functions and applications; see "IPv6 support" on page 148 for exploitation information that is pertinent if you choose to use the IPv6 support. Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for complete information on the IPv6 support of this release. It is a new publication and it introduces the design, concepts, and enablement considerations of using IPv6 support.
- All the IPv4 functions previously provided by z/OS Communications Server are still supported in this release. You may choose to keep using IPv4 addressing for all your applications. The functional enhancements described in this document pertain only to IPv4 addressing unless specifically identified to be IPv6.
- The contents of the PDS SEZALINK load library were moved to the PDS/E SEZALOAD load library. Therefore, you must replace the name SEZALINK with the name SEZALOAD. In addition, a RACF program profile is needed for SEZALOAD since SEZALOAD replaced SEZALINK.
- The SEZAHELP and AEZAHELP data sets were replaced with HELP and AHELP, respectively; therefore, you must replace the name TCPIP.SEZAHELP with the name SYS1.HELP and you must replace the name TCPIP.AEZAHELP with SYS1.AHELP.
- The distribution library AEZAMOD1 was replaced with PDSE, AEZAMODS; therefore, you must replace the name AEZAMOD1 with AEZAMODS.
- The ASSORTEDPARMS and KEEPALIVEOPTIONS statements will not be supported in future releases. These two statements are no longer necessary and the use of ASSORTEDPARMS in combination with xxxCONFIG statements can produce undesired results. Therefore, IBM strongly recommends using:

  - The GLOBALCONFIG, IPCONFIG, TCPCONFIG, and UDPCONFIG statements instead of the ASSORTEDPARMS statement. These other statements provide support for the parameters currently on the ASSORTEDPARMS statement.
  - The TCPCONFIG statement instead of the KEEPALIVEOPTIONS statement. The TCPCONFIG statement provides support for the parameters currently on the KEEPALIVEOPTIONS statement.
- NPF (Network Print Facility) was previously shipped in a separate FMID. In z/OS V1R4 Communications Server, NPF is merged into the base. This change will not affect your operations.
- In order to prevent abends when the TCP/IP stack is run with an out of date version of the message catalog, the TCP/IP stack now will verify that the message catalog is current. The TCP/IP stack will revert to issuing default messages when it determines that the message catalog is out-of-date or inaccessible. This change allows TCP/IP to continue processing even without a message catalog.
- The limit on the number of RCPTs in a single SMTP job is 3000. If you have more than 3000 RCPTs in a single SMTP job, the excessive RCPT commands will receive a failure reply code '552 Too many recipients'. Abend B37 can still occur if no more space is available on volume or if the volume table of contents (VTOC) is full.
- IPBCAST is a new LINK keyword that was added in z/OS V1R4 Communications Server for QDIO broadcast support. IPBCAST allows you to configure an OSA-Express in QDIO mode to send and receive broadcast packets. For example, customers wishing to run RIPv1 over OSA-Express in QDIO mode need this support because RIPv1 does not support multicast. The OSA-Express microcode must support broadcast in order for IPBCAST to have effect.

Sysplex Distributor enhancements

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

- "Sysplex-wide Dynamic Source VIPAs for TCP connections"
- "Sysplexports" on page 135
- "Sysplex Wide Security Association (SWSA)" on page 136

In addition, the Sysplex Distributor round-robin distribution function of z/OS V1R5 Communications Server is available in z/OS V1R4 Communications Server with APAR PQ76866. See "Sysplex Distributor round-robin distribution" on page 66 for details of this function.

Sysplex-wide Dynamic Source VIPAs for TCP connections

For clients outside a Parallel Sysplex, Sysplex Distributor provides a single-IP-address appearance to application instances spread across the Sysplex. It also distributes incoming work among the various instances. Many applications are part of a cooperative network of applications, and the Sysplex applications that serve as clients to end users may also have to initiate (client-like) outbound connection requests to cooperating applications. The SOURCEVIPA feature allows applications to attain independence of any physical adapter; however, SOURCEVIPA is limited to statically defined VIPAs within a stack. Different instances of the same application using Sysplex Distributor, and thus having a single IP address for inbound connection requests, will use different IP addresses for their outbound connection requests. These problems are resolved by allowing a

Dynamic VIPA (DVIPA) to be used as the source IP address for TCP applications and to have the Sysplex stacks collaborate on assigning ephemeral ports to prevent duplicate connection 4-tuples when the same Distributed DVIPA is used as the source address on multiple stacks. (The term *4-tuples* here refers to the source IP address, the source port, the destination IP address, and the destination port.) These solutions are provided in z/OS V1R4 Communications Server by Sysplex-wide Dynamic Source VIPAs for TCP connections and Sysplexports.

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

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

Restrictions

TCPSTACKSOURCEVIPA support is for TCP connections only.

What this change affects

- Application development
- Customization
- Operations
- Usability

Using this function

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

Table 88. Sysplex-wide Dynamic Source VIPAs for TCP connections

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

Sysplexports

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

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

Restrictions

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

Performance issues

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

What this change affects

- Application development
- Customization
- Operations
- Usability

Using this function

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

Table 89. Sysplexports

Task	Procedure	Reference
Enable Sysplexports allocation.	Perform the following steps: • Set up the EZBEPORT Coupling Facility Structure. • Code the SYSPLEXPORTS keyword on a VIPADISTRIBUTE statement.	*z/OS Communications Server: SNA Network Implementation Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Communications Server: IP Configuration Guide*

Sysplex Wide Security Association (SWSA)

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

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

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

For Sysplex Distributor, SWSA does the following:

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

Restrictions

The following restrictions apply:

- The distribution of IPSec tunnels with Sysplex Distributor requires the IPSec policy for the dynamic VIPA address to be defined at a connection or host based granularity.
- Specifying a subnet or range granularity is not supported.

- The distributor host and any backups must be at the z/OS V1R4 Communications Server level and only target hosts that are at the z/OS V1R4 Communications Server level are eligible for distributed IPSec tunnel traffic.
- All systems that are participating (distributor and targets) in IPSec traffic distribution must be running the same FMID level code.
- This feature does not apply to manual tunnels.

What this change affects

- Security
- Availability

Using this function

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

Table 90. Sysplex Wide Security Association (SWSA)

Task	Procedure	Reference
Enable IPSec tunnels to be moved during VIPA takeover or giveback and allow IPSec traffic to be distributed in a Sysplex Distributor environment.	Perform the following steps: 1. Define an EZBDVIPA structure in the CFRM policy and activate the policy. 2. In the TCP/IP profile, code the DVIPSEC subparameter on the FIREWALL parameter in the IPCONFIG statement. 3. Ensure that your IPSec policy is defined to be identical on any host that may take over the dynamic VIPA or that may be a target for a Sysplex Distributed workload.	*z/OS Communications Server: IP Configuration Reference*, *z/OS Communications Server: IP Configuration Guide*, and *z/OS Communications Server: SNA Network Implementation Guide*

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

Network access control

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

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

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

Restrictions

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

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

What this change affects

- Customization
- Operation
- Diagnosis
- System Security

Using this function

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

Table 91. Network access control

Task	Procedure	Reference
Activate Network Access Control Inbound.	Add an INBOUND parameter to the NETACCESS statement in TCPIP PROFILE.	*z/OS Communications Server: IP Configuration Guide*
Notify the TCP/IP stack of changes to SERVAUTH class.	RACLIST or REFRESH the SERVAUTH class. Reconfigure the net access security zone table by using the VARY TCPIP,,OBEYFILE command.	*z/OS Communications Server: IP Configuration Guide*

Fast Response Cache Accelerator (FRCA) access control

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

Restrictions

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

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

What this change affects

- Customization
- Diagnosis
- System Security

Using this function

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

Table 92. FRCA access control

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

Resolver enhancements

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

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

Refer to *z/OS Communications Server: IP Configuration Guide* for information about the new local host table and search order. Refer to *z/OS Communications Server: IP Configuration Reference* for information about the new resolver setup statements. See "IPv6 support for the resolver" on page 151 for updates that were made to the resolver specifically for IPv6 support.

Restrictions

None.

What this change affects

- Application Development

Using this function

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

Table 93. Resolver enhancements

Task	Procedure	Reference
Change the location of the global and default IPNODES files.	Create new global and default IPNODES files and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	*z/OS Communications Server: IP Configuration Reference*
Reread existing global and default IPNODES files.	Update existing global and default IPNODES files and issue the command MODIFY RESOLVER,REFRESH,SETUP=.	*z/OS Communications Server: IP Configuration Reference*

Table 93. Resolver enhancements (continued)

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

Managed System Infrastructure (msys) for Setup enhancement

msys for Setup was introduced in z/OS Communications Server V1R2. In z/OS V1R4 Communications Server, msys for Setup support was enhanced to include configuring a TN3270 Server and IP port reservations.

Restrictions

None.

What this change affects

- Customization
- Diagnosis
- System Security

Using this function

To take advantage of msys for Setup enhancement, perform the task shown in Table 94. Note that all configuration data saved in LDAP using msys for Setup support from a previous release is preserved and automatically migrated to the z/OS V1R4 Communications Server level.

Table 94. msys for Setup

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

OSA-Express Direct SNMP subagent support

For several releases, the Communications Server TCP/IP SNMP subagent has supported SNMP network management data for OSA-Express adapters. With z/OS V1R4 Communications Server, a new SNMP OSA-Express Direct subagent provided by the OSA product can be used with the Communications Server SNMP support to provide OSA-Express management data. This new subagent communicates directly with the OSA-Express adapters and does not require OSA/SF to retrieve the management data. The OSA-Express adapter management data currently supported by the Communications Server TCP/IP subagent will continue to be supported.

For a complete understanding of the OSA-Express management data provided by the different subagents, it is important to refer to the product specific publications.

For more information regarding the OSA-Express Direct subagent and its OSA-Express management data support, refer to *zSeries OSA-Express Customer's Guide and Reference*. For more information regarding the Communications Server TCP/IP subagent and its OSA-Express management data support, refer to *z/OS Communications Server: IP System Administrator's Commands*.

Restrictions

None.

What this change affects

- SNMP network management

Using this function

There are no z/OS V1R4 Communications Server exploitation tasks for the OSA-Express Direct SNMP subagent support.

Event trace enhancements

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

- IPv6 addresses can be specified on the IPADDR trace option keyword to execute traces on IPv6 addresses. See "IPv6 support for event trace enhancements" on page 155 for the exploitation procedure.
- Captured traces can be further analyzed in a variety of ways by using IPCS.
- Support is added for IPv4 address prefix.
- The SOCKAPI event trace option was removed from the 'ALL' group option.
- A new event trace option called ND is added for the z/OS V1R4 Communications Server Neighbor Discovery function.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

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

Table 95. Event trace enhancements

Task	Procedure	Reference
Filter the TCPIP event trace by a group of IPv4 addresses using an address prefix.	Append a slash followed by a numeric value (in the range of 1-32) for the IPv4 address prefix on the IPv4 address filter specified in either a SYS1.PARMLIB member or in a Trace CT™ command. For example, 192.48.32/24 allows addresses from 192.48.32.00 to 192.48.32.255 to be filtered.	*z/OS Communications Server: IP Diagnosis Guide*

Table 95. Event trace enhancements (continued)

Task	Procedure	Reference
Turn on the Neighbor Discovery (ND) trace option.	Add ND to the list of trace options to the component trace SYS1.PARMLIB member. This turns on the ND trace option at TCP/IP initialization. Issue a Trace CT command with OPTIONS=(ND) to turn on the ND trace option after TCP/IP initialization.	*z/OS Communications Server: IP Diagnosis Guide*

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

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

Restrictions

The following restrictions apply:

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

Dependencies

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

What this change affects

- Operations
- Usability

Using this function

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

Table 96. TCP/IP support for Simple Network Time Protocol (SNTP)

Task	Procedure	Reference
Synchronize (S)NTP clients with the ETR as the source.	Do the following: 1. Read and understand the SNTP chapters in *z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*. 2. Start SNTPD. Note that when restricting low port usage, the port used by SNTPD (default value of 123) should either be reserved for the name of the SNTPD start procedure or the PORT statement's SERVAUTH Security Access Facility (SAF) parameter used. 3. The server will always act in unicast mode. Based on command line invocation options, it will optionally also act in multicast and/or broadcast mode.	*z/OS Communications Server: IP Configuration Reference* and *z/OS Communications Server: IP Configuration Guide*

Netstat enhancements

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

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

  FORMAT/-M SHORT
  Displays the output in the existing IPv4 format.

  FORMAT/-M LONG
  Displays the output in the format that supports IPv6 addresses.

  These output control options allow the stack to be configured for IPv4-only operation (not IPv6-enabled), while still allowing you to modify programs that rely on Netstat output to update and test new versions of these programs with IPv6-enabled output from Netstat.
- A stack-wide output format parameter (FORMAT SHORT/LONG) can be specified on the IPCONFIG profile statement. It will instruct Netstat to produce output in one of the above formats. FORMAT SHORT is only applicable when the stack is not IPv6-enabled.
- In addition to the stack-wide FORMAT parameter, a Netstat command line option FORMAT/-M with keyword SHORT/LONG is supported to override the stack-wide parameter. Whenever a user specifies the Netstat command line format option, it will override the stack-wide format parameter on an IPv4-only stack.

See "IPv6 support for Netstat" on page 153 for updates that were made to Netstat specifically for IPv6 support. Refer to *z/OS Communications Server: IP System Administrator's Commands* for a complete description of the Netstat command.

Restrictions

None.

What this change affects

- Usability

Using this function

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

Ping enhancements

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

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

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

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

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

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

  Message identifiers for informational and error messages are still supported and are displayed based on the TSO PROFILE MSGID setting.
- For TSO PING to be authorized to use RAW sockets, you must update member IKJTSOxx in SYS1.PARMLIB by adding PING under AUTHCMD NAMES

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

The TSO PING and UNIX shell oping/ping commands are enhanced in z/OS V1R4 Communications Server to support IPv6 IP addresses. See "IPv6 support for Ping" on page 154 for more information.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

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

Table 97. Ping enhancements

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

Traceroute enhancements

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

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

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

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

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

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

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

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

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

The TSO TRACERTE and UNIX shell otracert/traceroute commands are enhanced in z/OS V1R4 Communications Server to support IPv6 IP addresses. See "IPv6 support for Traceroute" on page 154 for more information.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

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

Table 98. Traceroute enhancements

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

New VTAM start options to adjust the QDIO or iQDIO storage

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

OSA Express storage for read processing

Table 99. OSA Express: Amount of storage for read processing

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

HiperSockets storage for read processing

Table 100. HiperSockets: Amount of storage for read processing

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

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

The new options are as follows:

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

Refer to “New VTAM start options to adjust the QDIO or iQDIO storage” for more information regarding these new VTAM start options. Refer to *z/OS MVS Initialization and Tuning Reference* for information about reviewing and altering the IVTPRM00 parmlib member for CSM fixed storage. Refer to *SNA Resource Definition Reference* Information APAR ii13235 for additional CSM information.

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

Restrictions

None.

What this change affects

- Storage for read processing

Using this function

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

Table 101. New VTAM start options to adjust the QDIO or iQDIO storage

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

IPv6 support

Enabling IPv6 support

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

Migration considerations

Consider the following as you migrate:

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

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

- The limited IPv6 support of AF_INET6 in the BPXPRMxx NETWORK statement in Communications Server for OS/390 V2R10 was only at the TCP/IP layer. This means that the following was true in Communications Server for OS/390 V2R10:
  - The stack was not IPv6 enabled.
  - The Netstat reports were unchanged.

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

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

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

Restrictions

None.

What this change affects

- IPv6 application enablement and communication

Using this function

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

Table 102. Enabling IPv6 support

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

Configuration changes related to IPv6 support

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

Specifically, these are new or changed configuration statements:

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

The changed operator commands include the following:

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

Refer to *z/OS Summary of Message and Interface Changes* for information about the changes to statements and commands from release to release. Refer to *z/OS Communications Server: IP Configuration Guide* and to *z/OS Communications Server: IPv6 Network and Application Design Guide* for detailed discussion about IPv6 configuration considerations. Refer to *z/OS Communications Server: IP Configuration Reference* for details on the syntax of statements, parameters, and commands.

Restrictions

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

Incompatibilities

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

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

Dependencies

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

Using this function

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

Table 103. Configuration changes related to IPv6 support

Task	Procedure	Reference
Add an IPv6 route to the IP route table.	Specify BEGINROUTES with an IPv6 address.	*z/OS Communications Server: IP Configuration Reference*
Control packet tracing for IPv6 address.	Specify one of the following with an IPv6 address: • PKTTRACE statement • V TCPIP,,PKTTRACE command	*z/OS Communications Server: IP Configuration Reference*
Trace socket data for IPv6 address.	Specify V TCPIP,,DATTRACE with an IPv6 address.	*z/OS Communications Server: IP Configuration Reference*
If the stack is not enabled for IPv6, display command output as if it could contain IPv6 addresses.	Specify IPCONFIG FORMAT LONG.	*z/OS Communications Server: IP Configuration Reference*
Enable IPv6 forwarding.	Specify IPCONFIG6 DATAGRAMFWD.	*z/OS Communications Server: IP Configuration Reference*
Enable multipath route selection for IPv6.	Specify IPCONFIG6 MULTIPATH PERPACKET or IPCONFIG6 MULTIPATH PERCONNECTION.	*z/OS Communications Server: IP Configuration Reference*
Ignore ICMPv6 redirects.	Specify IPCONFIG6 IGNOREREDIRECT.	*z/OS Communications Server: IP Configuration Reference*
Enable IPv6 Source VIPA support.	Specify IPCONFIG6 SOURCEVIPA and code the SOURCEVIPAINT keyword on an IPv6 INTERFACE statement.	*z/OS Communications Server: IP Configuration Reference*
Set IPv6 hop limit.	Specify IPCONFIG6 HOPLIMIT.	*z/OS Communications Server: IP Configuration Reference*

Table 103. Configuration changes related to IPv6 support (continued)

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

IPv6 support for the resolver

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

- New resolver APIs are introduced for IPv6 enabled applications.

  The new APIs, Getaddrinfo and Getnameinfo, allow applications to query host names for IPv6-enabled hosts and IPv6 addresses. The APIs also allow the application to optionally query a server's port and protocol. These APIs also allow the application to optionally query a server's port and protocol. A third new API, Freeaddrinfo, works in conjunction with Getaddrinfo to provide a thread safe environment.

  Refer to the discussion on resolver enhancements in *z/OS Communications Server: IPv6 Network and Application Design Guide* for more information.
- New DNS resource records are defined to represent hosts with IPv6 addresses. This changes the contents of network flows between resolvers and name servers.

  See "BIND-based DNS name server" on page 169 for more information about the DNS IPv6 support.
- The resolver uses an RFC defined algorithm to sort addresses returned for a multi-homed host.

  Refer to the discussion on Default Address selection-Destination address selection in *z/OS Communications Server: IPv6 Network and Application Design Guide* for information about the sorting algorithm utilized by the resolver's Getaddrinfo processing.
- New local host table support. This introduces:
  - A new type of local host table, IPNODES.

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

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

Restrictions
None.

What this change affects
- Application Development

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

Table 104. IPv6 support for resolver

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

IPv6 support for applications
The following applications support IPv6:
- FTP server and FTP client – see "IPv6 support for FTP" on page 162 for more information.
- Inetd server
- Otelnetd server
- Orshd server
- Orexecd server
- UNIX rexec client
- Netstat – see "IPv6 support for Netstat" on page 153 for more information.

- TSO/UNIX Traceroute – see "IPv6 support for Traceroute" on page 154 for more information.
- TSO/UNIX Ping – see "IPv6 support for Ping" on page 154 for more information.

Restrictions
None.

What this change affects
- Usability

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

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

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

See "Netstat enhancements" on page 143 for updates to Netstat in z/OS V1R4 Communications Server that are not related to IPv6 support. Refer to *z/OS Communications Server: IP System Administrator's Commands* for a complete description of the Netstat command.

Restrictions
None.

What this change affects
- Diagnosis
- Operations
- Usability

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

Table 105. IPv6 support for Netstat

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

IPv6 support for Ping

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

See "Ping enhancements" on page 144 for updates to Ping in z/OS V1R4 Communications Server that are not related to IPv6 support.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

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

Table 106. IPv6 support for Ping

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

IPv6 support for Traceroute

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

See "Traceroute enhancements" on page 145 for updates to Traceroute in z/OS V1R4 Communications Server that are not related to IPv6 support.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

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

Table 107. IPv6 support for Traceroute

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

IPv6 support for IPv6 IPCS subcommands formatting

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

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

Refer to *z/OS Summary of Message and Interface Changes* for information about the changes to statements and commands from release to release. Refer to *z/OS Communications Server: IP Diagnosis Guide* for details on TCPIPCS subcommands.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

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

IPv6 support for event trace enhancements

In z/OS V1R4 Communications Server, the event trace functions are enhanced for IPv6 by allowing IPv6 addresses to be specified on the IPADDR trace option keyword to execute traces on IPv6 addresses. There are also IPv4 enhancements associated with event tracing; see "Event trace enhancements" on page 141 for details.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

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

Table 108. IPv6 support for event trace enhancements

Task	Procedure	Reference
Filter the TCPIP event trace by IPv6 addresses.	Code the IPv6 addresses (and optionally numeric IPv6 address prefixes) on the IPADDR keyword by specifying one of the following: • The component trace SYS1.PARMLIB member CTIEZBxx • The Trace CT command	*z/OS Communications Server: IP Diagnosis Guide*
Turn on the Neighbor Discovery (ND) trace option.	Add ND to the list of trace options to the component trace SYS1.PARMLIB member. This turns on the ND trace option at TCP/IP initialization. Issue a Trace CT command with ″OPTIONS=(ND)″ to turn on the ND trace option after TCP/IP initialization.	*z/OS Communications Server: IP Diagnosis Guide*

IPv6 support for RAS packet trace and data trace

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

Restrictions

None.

What this change affects

- Diagnosis

Using this function

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

IPv6 support for socket API commands

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

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

Refer to *z/OS Communications Server: IPv6 Network and Application Design Guide* for more detailed information about IPv6 support for TCP/IP socket API commands.

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

Restrictions

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

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

What this change affects

- Application Development

Using this function

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

Table 109. IPv6 support for TCP/IP socket API commands

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

FTP support for substitution characters during EBCDIC/ASCII single-byte translations

Prior to this release, if a character in the input stream did not map to the file system code set during a file transfer, FTP would fail the transfer. z/OS V1R4 Communications Server allows you to configure FTP to use substitution characters for non-translatable characters, thus avoiding failed transfers.

Restrictions

If a substitution occurs during a file transfer, you cannot restore the original file by reversing the order of file transfer.

What this change affects

- Operations

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 110. FTP support for substitution characters during EBCDIC/ASCII single-byte translations

Task	Procedure	Reference
Enable FTP to substitute characters that cannot be translated.	In FTP.DATA, specify SBSUB TRUE.	*z/OS Communications Server: IP Configuration Reference*
Specify the single-byte substitution character in a hexadecimal format that will be used for substitution.	In FTP.DATA, specify a single-byte character, in a hexadecimal format, to a SBSUBCHAR keyword.	*z/OS Communications Server: IP Configuration Reference*

Table 110. FTP support for substitution characters during EBCDIC/ASCII single-byte translations (continued)

Task	Procedure	Reference
After logging in to FTP, enable FTP to substitute for characters that cannot be translated (for the current session only).	Perform the following steps: • Issue SITE and LOCSITE subcommands with the SBSUBCHAR parameter to specify the substitution character. • Issue SITE and LOCSITE subcommands with the SBSUB=TRUE parameter.	*z/OS Communications Server: IP User's Guide and Commands*

Enhanced FTP activity logging

In z/OS V1R4 Communications Server, the FTP server is enhanced with improved diagnostic information recorded in the SYSLOGD file. The information uses message numbers that are documented in *z/OS Communications Server: IP Messages Volume 3 (EZY)* and allows for correlation of information recorded for an FTP session. The enhanced FTP activity logging provides the system programmer with standardized information for resolving FTP problems and for tracking usage of the services of the FTP server.

Restrictions

None.

Dependencies

SYSLOGD must be started.

What this change affects

- Diagnosis

Using this function

This function does not require any action unless you want to take advantage of the function. If so, perform the appropriate task in the following table.

Table 111. Enhanced FTP activity logging

Task	Procedure	Reference
Request activity logging for non-anonymous users.	In the FTP.DATA file for the server, code: FTPLOGGING TRUE.	*z/OS Communications Server: IP Configuration Reference*
Request activity logging for anonymous users.	In the FTP.DATA file for the server, code: ANONYMOUSFTPLOGGING TRUE.	*z/OS Communications Server: IP Configuration Reference*

Changed behavior of login failure replies

z/OS V1R4 Communications Server changes the default behavior of password failure replies. When the PASS command fails, the FTP server will now reply to the client with minimal information about why the PASS command failed. This is an enhancement to the previous behavior because this change prevents sensitive information about USERIDs and PASSWORDS from being exposed to the end user.

Note: This update is available in z/OS V1R2 Communications Server with APAR PQ51780.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

This update does not require any action. The change is automatic (the default for the FTP.DATA keyword ACCESSERRORMSGS is FALSE). If you want to override the default and reply to the client with detailed PASS command failure information, perform the first task in the following table. If you want to prevent password failure information from being returned to the client, yet record error information for diagnostic purposes, then perform the second task in the table.

Table 112. Changed behavior of login failure replies if you want to override default behavior

Task	Procedure	Reference
Override the new default behavior and obtain detailed information for password failure replies.	Do one of the following: • Configure the FTP server to send additional information by setting the FTP.DATA keyword ACCESSERRORMSGS to TRUE. This will send detailed login failure information that includes the function call that failed and its return and reason code. • Turn on the DEBUG option called ACC to log the error messages in the syslog.	*z/OS Communications Server: IP Configuration Reference*
Prevent password failure information from being returned to the client, yet record error information for diagnostic purposes.	Turn on the DEBUG option ACC to log the error information in the syslog.	*z/OS Communications Server: IP Diagnosis Guide* and *z/OS Communications Server: IP Configuration Reference*

Support for Chinese standard GB18030 provided by codepage IBM-5488

z/OS V1R4 Communications Server allows FTP to transfer files that are encoded in the IBM-5488 codepage.

Restrictions

The support requires that the following FTP protocols are in use at the time of a data transfer:

Protocol	Type
Structure	FILE
Transmission mode	STREAM
Data type	ASCII

In addition, the following additional restrictions are enforced when the support is used:

- The FILETYPE setting must be SEQ.
- If the file transferred is an MVS data set, its record format (RECFM) must be V, VB, or U.

- If the file transferred is an MVS data set with RECFM=V or RECFM=VB and the transfer is outbound, then requesting RDWs is not allowed.
- For the FTP server, the SIZE command is not allowed.
- For the FTP client, the transfer must not be part of the SRESTART subcommand.

What this change affects

- Customization

Using this function

The support for Chinese standard GB18030 provided by codepage IBM-5488 function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 113. Support for Chinese standard GB18030 provided by codepage IBM-5488

Task	Procedure	Reference
Choose the IBM-5488 codepage for the FTP server's data connection translate table.	In the server's FTP.DATA file, code ENCODING MBCS and code MBDATACONN (IBM-1388,IBM-5488).	*z/OS Communications Server: IP Configuration Reference*
Choose the IBM-5488 codepage for the FTP client's data connection translate table.	In the client's FTP.DATA file, code ENCODING MBCS and code MBDATACONN (IBM-1388,IBM-5488).	*z/OS Communications Server: IP User's Guide and Commands*
Change data connection translation tables to the IBM-5488codepage during an FTP client/server session.	Change server's translation table by issuing SITE ENCODING=MBCS and by issuing SITE MBDATACONN=(IBM-1388,IBM-5488). Change client's translation table by issuing LOCSITE ENCODING=MBCS and by issuing LOCSITE MBDATACONN=(IBM-1388,IBM-5488).	*z/OS Communications Server: IP User's Guide and Commands*

Enhancements to FTP server user exits

z/OS V1R4 Communications Server allows FTP exits to support IPv6 local and remote addresses and also allows implementation of more comprehensive FTP server security exit functions. The following enhancements to FTP user exits are introduced:

- New samples are provided for all exits.

  The new samples of all the changed exits are provided in SEZAINST. The samples FTCHKCM1 and FTCHKCM2 are also updated. The SEZAINST(FTPOSTPR) exit was added in Communications Server for OS/390 V2R10 in the C language. In z/OS V1R4 Communications Server, a new sample called SEZAINST(FTPOSTPA) is included in the Assembler language.
- Bytes transferred and data set name are now passed to FTPOSTPR.
- Client and server IP addresses now include support for IPv6 addresses in all exits except FTPSMFEX user exit. The FTPSMFEX user exit is unchanged because it utilizes the old SMF Type 118 record instead of the preferred SMF Type 119 record.
- A scratchpad area is available for communicating between exits.

  The 256-byte scratchpad area can be used to communicate between the exits that have access to it. It is not altered by FTP after its initial allocation and it persists

as long as the session for this user remains active. The contents are lost if the session switches to a new userid or logs off. It may contain any data within the 256 bytes. Some potential uses for the scratchpad are counting the number of attempts by a user to access a resource, passing information from one exit to another to control processing, or even using STCK to time the execution of a command.

The following table provides a list of the parameters and the exits that are affected.

Table 114. FTP parameters and user exits that are enhanced in z/OS V1R4 Communications Server

Parameter	User Exit
Buffer to hold 500- reply extension	FTCHKCMD
Number of bad passwords in this login attempt	FTCHKPWD
Name of data set or HFS file stored or retrieved	FTPOSTPR
Total bytes transferred	FTPOSTPR
Scratchpad buffer to communicate with other exits	FTCHKCMD, FTCHKJES, FTPOSTPR
Client's socket address structure	All but FTPSMFEX
Server's socket address structure	All but FTPSMFEX
Session instance identifier used in logging messages for this session	All but FTPSMFEX

Restrictions

The following restrictions apply:

- The z/OS V1R4 Communications Server enhanced FTP user exit interface is compatible with user exits from prior releases. The old user exits can run as is, or they can be modified to take advantage of the z/OS V1R4 Communication Server parameters. FTCHKIP and FTPOSTPR may continue to reference their existing IP address fields for IPv4 addresses and IPv4 addresses mapped into IPv6 format. Once the exits are used with true IPv6 addresses, the new socket address structure parameters must be used instead.
- The two user exits that are loaded prior to the spawning of the final process (FTCHKIP and FTCHKPWD) will not have access to the scratchpad. FTCHKCMD, FTCHKJES and FTPOSTPR will have access to the scratch pad during USER/PASS commands, but the contents will be reset after the USER/PASS processing.

What this change affects

- Customization
- Installation
- Security
- Usability

Using this function

The enhancements to FTP server user exits do not require any action unless you want to take advantage of the new information passed to the exits. If so, perform the tasks in the following table.

Table 115. Enhancements to FTP server user exits

Task	Procedure	Reference
Modify existing exits to use the new interface (required only to use the new parameters).	Use the provided samples for each exit to update the calling parameter list for each exit and to access the new parameters in the list.	*z/OS Communications Server: IP Configuration Reference* and SEZAINST sample library
Modify exits to utilize the new parameters.	Use the provided samples or your modified exits as a base. To these exits, add instructions that make decisions based on the new parameters, such as rejection of login based on IP address, tracking number of bytes for all transfers, and customizing a 500- reply to explain why a command was rejected by FTCHKCMD.	*z/OS Communications Server: IP Configuration Reference*, *z/OS MVS Programming: Authorized Assembler Services Guide*, and SEZAINST sample library
Ensure proper authorization.	The user exit load modules must be placed in an APF-authorized library to which the FTP server has access by way of STEPLIB, linklist, or LPA. Also, the authorization state (JSCBAUTH) must be the same after exiting from the user exit as it was upon entry. If a user exit is not found, processing proceeds as though a return code of 0 was received from the user exit call.	*z/OS Communications Server: IP Configuration Reference* and *z/OS MVS Initialization and Tuning Reference*

IPv6 support for FTP

Prior to this release, a z/OS FTP client could not communicate with an FTP server on an IPv6 node, nor could the z/OS FTP server accept connections from clients executing on IPv6 nodes. In z/OS V1R4 Communications Server, IPv6 support is added to FTP to make IPv6 connectivity possible for both the FTP client and server.

RFC 2428 implementation is part of the IPv6 enhancement.

Restrictions

The following restrictions apply:

- The FTP client SOCKSCONFIGFILE is never referenced by the client when connecting to an FTP server with an IPv6 IP address.
- In the SOCKSCONFIGFILE, you cannot specify the DNS name of a SOCKS server on an IPv6 node unless the IPv6 node is multihomed and accessible from an IPv4 network.
- Proxy transfer between mixed protocol FTP servers (that is, between a server known to the FTP client as an IPv6 node and a server known to the FTP client as an IPv4 node), will succeed only if the primary server can connect to the secondary server using the same protocol as the secondary server's control connection.
- The FTP server does not allow the EPSV command to specify a protocol for the data connection different from the protocol used for the control connection.
- The FTP server does not allow the EPRT command to specify a protocol for the data connection different from the protocol used for the control connection.
- The FTP server does not accept the PORT command when the control connection is IPv6.

- Kerberos protection of IPv6 connections is not supported by either client or server.
- For IPv6 connection partners, RACF does not validate the login. RACF does not prevent any IPv6 connection partner from accessing the server.

Incompatibilities

z/OS FTP will not be able to use IPv6 connections unless at least one TCP/IP stack on your system supports IPv6 networking. The z/OS TCP/IP stack does not support IPv6 networking unless you define it to UNIX System Services as an AF_INET6 network.

Dependencies

To use this function, you must have an IPv6 enabled TCP/IP, such as z/OS V1R4 TCP/IP configured as an AF_INET6 network.

What this change affects

- Operations
- Availability
- Diagnosis
- Usability

Using this function

This function does not require any action unless you want your FTP server or client to operate with IPv6 networks. If so, perform the tasks in the following table.

Table 116. IPv6 application for FTP

Task	Procedure	Reference
Enable FTP server to accept connections from IPv6 nodes as well as IPv4 nodes.	Configure z/OS TCP/IP (or any other TCP/IP stack) as an AF_INET6 network.	*z/OS Communications Server: IPv6 Network and Application Design Guide*
Enable FTP client to connect to FTP server on an IPv6 node.	Do the following: 1. Configure client host z/OS TCP/IP (or any other TCP/IP stack) as an AF_INET6 network. 2. Update hostname files to define host names for IPv6 server hosts (This is optional. You can always specify the FTP server as an IP address instead of a host name).	*z/OS Communications Server: IPv6 Network and Application Design Guide*, *z/OS Communications Server: IP Configuration Reference*, and *z/OS Communications Server: IP Configuration Guide*
Connect to FTP server on an IPv6 node.	Use FTP client foreign-host start option, or use the OPEN subcommand hostname parameter, to specify the IPv6 FTP server.	*z/OS Communications Server: IP User's Guide and Commands*

Port qualification by linkname or destination IP address

When multiple TCPIP stacks are consolidated, the Telnet port is usually the same on all the original stacks but the stacks have different parameters and mapping statements. In the past, the only consolidation solution was to create new port numbers to retain the different characteristics of the multiple Telnets. The end users had to be notified of the port number change and they were required to make the changes. With port qualification, the end users can all use the same port

as long as the original destination addresses are all moved into the consolidated TCPIP stack. Specifically, z/OS V1R4 allows a single port to have different Telnet characteristics based on the destination IP address or linkname.

Refer to *z/OS Communications Server: IP Configuration Guide* for more information about port qualification.

Restrictions

None.

What this change affects

- Customization

Using this function

If you want to take advantage of the port qualification by linkname or destination IP address, perform the task in the following table.

Table 117. Port qualification by linkname or destination IP address

Task	Procedure	Reference
Qualify the port to be used.	If a port qualifier is used, you must specify it on both the TelnetParms and BeginVTAM statements. Specify the nnn,port_qual option on the Telnet Port and SecurePort statements. Specify the nnn,port_qual option on the BeginVTAM Port statement.	*z/OS Communications Server: IP Configuration Reference*

Printer enhancements

In z/OS V1R4 Communications Server, printer specification is enhanced in two ways:

- You can specify a default application for printer connections.
- You can specify whether or not the printer session should be dropped when the terminal session is dropped.

  Prior to this enhancement, when the terminal emulator partner of an associated printer was dropped, the printer session remained active and the terminal LU was available for the next connection. This could potentially cause a problem for a new user.

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

Restrictions

None.

What this change affects

- Customization

Using this function

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

Table 118. Telnet printer enhancements

Task	Procedure	Reference
Specify a default application for printer connections.	Code the new BeginVTAM statement PRTDEFAULTAPPL.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Specify whether or not the printer session should be dropped when the terminal session is dropped.	Code DROPASSOCPRINTER. It is allowed in the TelnetGlobals, TelnetParms, and the ParmsGroup statement blocks.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Parameter placement enhancements

In z/OS V1R4 Communications Server, parameters are enhanced in the following ways:

- Most parameters are now available in all three information blocks: the TelnetGlobals, TelnetParms, and the ParmsGroup.
- The TelnetDevice statement can now be coded as a parameter in TelnetGlobals, TelnetParms, and the ParmsGroup information blocks. This allows for more granularity when assigning logmodes.
- A PMAP prmgrp_name option is added for the LUMAP and PRTMAP statements to map a ParmsGroup to an LU group. With this addition, parameters can be assigned based on the LU name or group chosen.

Note: A few parameters (LuSessionPend, MSG07, TelnetDevice) can now be coded in both BeginVTAM and as a parameter in the TelnetGlobals, TelnetParms, or ParmsGroup information blocks. Warning messages will be issued when these Telnet parameters are used in BeginVTAM indicating the use is accepted but the preferred placement is in one of the parameter blocks. In a future release, the BeginVTAM placement will not be allowed.

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

Restrictions

None.

What this change affects

- Customization

Using this function

None.

New DEBUG option to suppress the connection dropped error messages

In z/OS V1R4 Communications Server, a new DEBUG option called EXCEPTION allows the system administrator to turn off all but exception debug messages. This is similar to the OFF option in z/OS V1R2 Communications Server. In z/OS V1R4 Communications Server, the OFF option is changed to turn off all debug messages. This includes the CONN DROP for error or timeout that are not suppressed by DEBUG EXCEPTION.

DEBUG EXCEPTION is the default in z/OS V1R4 Communications Server.

Restrictions

None.

What this change affects

- Customization

Using this function

DEBUG EXCEPTION is the default in z/OS V1R4 Communications Server. If you coded DEBUG OFF in previous releases and you now want exception messages to be issued, perform the task in the following table.

Table 119. DEBUG EXCEPTION option

Task	Procedure	Reference
Turn off all debug messages except the connection dropped error messages.	Code the new EXCEPTION option on the DEBUG statement.	*z/OS Communications Server: IP Configuration Reference*

New QINIT option for default applications

When an end user logs off an application that is defined as a LOGAPPL application, the normal response of Telnet is to send a USSMSG10 or solicitor screen to the end user. z/OS V1R4 Communications Server introduces a new QINIT option as a mutually exclusive alternative to LOGAPPL on the DEFAULTAPPL, PRTDEFAULTAPPL, LUMAP-DEFAPPL, and PRTMAP-DEFAPPL statements. The QINIT option allows Telnet to reestablish the session when logging off the LOGAPPL application instead of sending a USSMSG10 or solicitor screen. Specifying the QINIT option instead of LOGAPPL therefore allows you to use LOGAPPL function while keeping the original behavior of DEFAULTAPPL or DEFAPPL.

Restrictions

None.

What this change affects

- Customization

Using this function

If you want to take advantage of the new QINIT option, perform the task in the following table.

Table 120. Default application QINIT option

Task	Procedure	Reference
Use the function provided by LOGAPPL while keeping the original behavior of DEFAULTAPPL or DEFAPPL.	Specify QINIT on the DEFAULTAPPL, PRTDEFAULTAPPL, LUMAP-DEFAPPL, and PRTMAP-DEFAPPL statements. It is a mutually exclusive alternative to LOGAPPL.	*z/OS Communications Server: IP Configuration Reference*

LU mapping enhancements

z/OS V1R4 Communications Server introduces the following enhancements that are related to LU mapping:

- Telnet can now be instructed to use sequential LU name lookup or select the first LU available in the pool each time. Sequential LU lookup is the default method in z/OS V1R4 Communications Server. The z/OS V1R2 Communications Server and earlier default method was to select the first LU available each time.
- Telnet wildcard capability has been expanded beyond numeric or alphabetic range specification. Now each individual character position can be defined as Fixed, Numeric, Alphabetic, Alphanumeric, Hexadecimal, or as a wildcard.
- LU names can be retained (or kept) for a specified period of time after the name has been released. While in the kept state, only the same Client Identifier can reconnect and use the same name again. To all other Client Identifiers the LU name will not be available. Once the specified keep time is reached, any Client Identifier can be assigned the LU.
- Capacity checks can now be specified for LU or PRT groups. When the in-use number reaches the capacity check limit, defined as a percentage of the total, a message will be issued warning that the LU pool is reaching its limit.
- LU naming exits can be written by the system administrator. Instead of defining the LU names in an LU or PRT group, the system administrator can identify the group as an exit and assign the same name as the exit assembler program. The group is defined as an exit in Telnet. When Telnet performs LU lookup, it will call the exit routine that was loaded during profile processing and let the exit generate an LU name.

Restrictions

None.

What this change affects

- Customization

Using this function

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

Table 121. LU mapping enhancements

Task	Procedure	Reference
Specify Sequential LU name lookup method.	Specify the SequentialLU|NoSequentialLU parameter statement. It is available in the TelnetGlobals, TelnetParms, and ParmsGroup statement blocks.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Keep an LU name for a period of time after the name has been released.	Specify the KeepLU parameter statement. It is available in the TelnetGlobals, TelnetParms, and ParmsGroup statement blocks.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Perform a capacity check for LU or PRT groups.	Specify a capacity percentage on LUGROUP and PRTGROUP statements.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Table 121. LU mapping enhancements (continued)

Task	Procedure	Reference
Write LU naming exits.	Code LU exit routines to validate or select an LU name used to represent the client. The entry point name must match the routine name specified as the LUGROUP group name. Each LU exit routine specified must be assembled and link-edited as a stand-alone load module.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*

Upgrade TN3270 SSL to use TLS

In z/OS V1R4 Communications Server, TN3270 is upgraded to support the TLS V1 protocol for secure connections.

Restrictions

The TN3270 client must also support TLS.

What this change affects

- Customization

Using this function

There are no migration procedures associated with this function. No changes are required. If a TN3270 client requests TLS, a TLS protected session will be started. The display Telnet connection detail report is updated to include the protocol (SSLV2, SSLV3, TLSV1) that is in use for the connection.

This section describes the updates to SNMP introduced in z/OS V1R4 Communications Server.

SNMP agent

The SNMP agent allows you to provide some initial settings for a small set of MIB objects by using the OSNMPD.DATA file. One of the objects for which an initial value can be provided is sysObjectID.0. The sysObjectID.0 object is the vendor's authoritative identification of the network management subsystem contained in the entity. That is, it is intended to uniquely identify the SNMP agent. Changing this value is not recommended and will be disabled in a subsequent release. In z/OS V1R4 Communications Server, warning message EZZ6317I will be issued if the object is set by using the OSNMPD.DATA file.

SNMP TCP/IP subagent

In z/OS V1R4 Communications Server, the SNMP TCP/IP subagent supports both IPv4 and IPv6 processing for the TCP scalar counter MIB objects from RFC 2012 and the UDP scalar counter MIB objects from RFC 2013. Also, some of the outbound ICMP counters were previously only incremented for those ICMP messages that the TCP/IP stack initiated. As of z/OS V1R4 Communications Server, all the outbound ICMP counters will now also be incremented for those ICMP messages sent by the TCP/IP stack at the request of an application. The BIND 9 name server was introduced in z/OS V1R2 Communications Server. In z/OS V1R4 Communications Server, the BIND 9 name server is upgraded to the BIND 9.2 level. This allows DNS communications from server-to-server and from client- (utilities and resolvers) to-server over IPv6 connections, with additional

configuration options relating to IPv6 connections and server tuning. The z/OS V1R2 Communications Server version of the name server supported IPv6 resource records, but was unable to communicate over IPv6.

With BIND 9.2, resolvers are able to receive complete and accurate DNS responses for some types of IPv6 queries because BIND 9.2 includes support for A6 and DNAME chaining on behalf of resolvers that do not support such chaining. Note that BIND 9.1 did not support resolution of resource record through record chaining on behalf of a resolver.

For more information on A6 chaining, see the section that discusses address lookups using A6 records in *z/OS Communications Server: IP Configuration Guide*.

BIND-based DNS name server

The BIND 9 name server was introduced in z/OS V1R2 Communications Server. In z/OS V1R4 Communications Server, the BIND 9 name server is upgraded to the BIND 9.2 level. This allows DNS communications from server-to-server and from client- (utilities and resolvers) to-server over IPv6 connections, with additional configuration options relating to IPv6 connections and server tuning. The z/OS V1R2 Communications Server version of the name server supported IPv6 resource records, but was unable to communicate over IPv6.

With BIND 9.2, resolvers are able to receive complete and accurate DNS responses for some types of IPv6 queries because BIND 9.2 includes support for A6 and DNAME chaining on behalf of resolvers that do not support such chaining. Note that BIND 9.1 did not support resolution of resource record through record chaining on behalf of a resolver.

For more information on A6 chaining, see the section that discusses address lookups using A6 records in *z/OS Communications Server: IP Configuration Guide*.

Dependencies

In order for the BIND 9 name server to perform A6 chain resolution for DNS A6 resource records on behalf of resolvers that do not support A6 chain resolution, the BIND 9 name server must be configured with the *allow-v6-synthesis* option in named.conf.

Restrictions

None.

What this change affects

- Customization
- Diagnosis
- Operations
- Performance
- Storage

Configuration file updates

BIND 9 DNS configuration file (named.conf)

The following updates were made to the BIND 9 DNS configuration file (named.conf) in z/OS V1R4 Communications Server:

- The unmatched category has been added to the logging{} statement.
- The forwarders option now accepts an optional port.
- The allow-v6-synthesis option was added to the options{} statement and view statements.

  Note: This option was made obsolete in z/OS V1R5 Communications Server.
- The serial-query-rate option was added to the options{} statement.
- The random-device option was added to the options{} statement.
- The max-cache-size option was added to the options{} statement.
- The minimal-responses option was added to the options{} statement.
- The listen-on-v6 option was added to the options{} statement.
- The query-source-v6 option was added to the options{} statement.
- The transfer-source-v6 option was added to the options{} and zone{} statements.
- The notify-source-v6 option was added to the options{} and zone{} statements.
- The max-buffered-messages option was added to the options{} statement.
- The match-mapped-addresses option was added to the options{} statement.
- The edns option was added to the server{} statement.
- The $GENERATE directive now supports DNAME records.
- The behavior of the controls{} statement has changed. rndc may be used without a controls{} statement under the proper circumstances. Also, the keys clause of the controls{} statement is now optional.
- Root hints are now fully optional. For class IN views, a compiled-in hints file will be used by default. For non-IN class views, there is no compiled-in default hints file and such views can provide authoritative services, but not recursion.
- ACL names are no longer case sensitive.
- Configuration files no longer have reserved words.
- The default TTL for BIND 9 zones has changed. BIND 9 strictly complies with the RFC 1035 and RFC 2308 rules regarding omitted TTLs in zone files. Omitted TTLs are replaced by the value specified with the $TTL directive, or by the previous explicit TTL if there is no $TTL directive.

  If there is no $TTL directive and the first RR in the file does not have an explicit TTL field, the zone file is illegal according to RFC 1035 because the TTL of the first RR is undefined. Unfortunately, BIND 4 and many versions of BIND 8 accept such files without warning and use the value of the SOA MINTTL field as a default for missing TTL values. The BIND 9 name server in z/OS V1R2 Communications Server did not load such files. The BIND 9 name server in z/OS V1R4 Communications Server emulates the nonstandard BIND 4/8 SOA MINTTL behavior and loads the files (provided that the SOA is the first record in the file), but will issue the warning message ″no TTL specified; using SOA MINTTL instead″.

  To avoid problems, IBM recommends that you use a $TTL directive in each zone file.
- The BIND 9 name server logging has changed slightly. If the logging level is chosen as 'debug' and the debug level is omitted, the default debug level is now 1 instead of 0.
- When a size limit is associated with a log file, it will only be rolled when the size is reached, not every time the log file is opened. For example, the log files will no longer be automatically rolled if the name server is stopped and restarted.
- Options that accepted IPv4 addresses now also accept IPv6 addresses.

- Prior to z/OS V1R4 Communications Server, some options that were inappropriate for a given type of zone were ignored. As of z/OS V1R4 Communications Server, these types of errors are no longer ignored and they cause an error message to be issued and the name server to end. Refer to the table for named.conf options and valid zone types in *z/OS Communications Server: IP Configuration Reference*. It lists the options that will undergo this enforcement and lists the types of zones for which they are valid.
- The print-category, print-severity, and print-time logging options have had their default value changed from *no* to *yes*.
- The print-threadid logging option is new.

rndc.conf configuration file

The following changes were made to the rndc.conf configuration file in z/OS V1R4 Communications Server:

- rndc configuration may be done automatically, under the proper circumstances, with the creation of a rndc.key file by the BIND 9 name server. See Table 123 on page 172 for details.
- The port and default-port clauses are new to the rndc.conf file.

Refer to *z/OS Summary of Message and Interface Changes* for more information about changes to configuration files.

UNIX command updates

Updates were made to the following UNIX commands in z/OS V1R4 Communications Server for DNS:

- dig
- named
- rndc

In addition, a new UNIX command was introduced in z/OS V1R4 Communications Server for DNS:

- rndc-confgen

Refer to *z/OS Summary of Message and Interface Changes* for details about all updates to UNIX commands for DNS.

Using this function

If you want to run the name server using the BIND 9.2 upgrades, perform the tasks in the following table.

Table 122. BIND 9.2 upgrades

Task	Procedure	Reference
Allow the name server to communicate over IPv6 (optional).	Specify the *listen-on-v6* option in named.conf. You may also specify IPv6 addresses in access control lists, server statements, masters clause in slave zone statement, and any other options that specify IP addresses.	*z/OS Communications Server: IP Configuration Reference*
Add IPv6 information to the name server (optional).	Add IPv6 records and/or zones to the name server configuration file and/or existing zone files.	*z/OS Communications Server: IPv6 Network and Application Design Guide*

Table 122. BIND 9.2 upgrades (continued)

Task	Procedure	Reference
Enable A6 Chain Resolution for Resolvers that are unable to perform A6 Chain Resolution on their own. (optional).	Specify the *allow-v6-synthesis* option in the named.conf file. Specify the addresses of the resolvers this option will apply to in the Access Control List (ACL).	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Limit cache storage size if desired. (optional).	Specify the *max-cache-size* option in the named.conf file.	*z/OS Communications Server: IP Configuration Reference*
Ensure syslogd is running.	Start the Syslog Daemon.	*z/OS Communications Server: IP Configuration Guide*
Start the BIND 9 name server with the new options.	Start the BIND 9 name server start procedure or start from the z/OS UNIX shell with the *named* command.	*z/OS Communications Server: IP System Administrator's Commands*
Check for errors.	Check the syslog output file and named log files for errors or warnings. Query the name server with *dig* or *nslookup* to further test the name server configuration.	*z/OS Communications Server: IP Diagnosis Guide*, *z/OS Communications Server: IP Messages Volume 4 (EZZ-SNM)*, and *z/OS Communications Server: IP System Administrator's Commands*
Be aware that updates were made to the BIND 9 DNS configuration file (named.conf). For example, the default TTL for BIND 9 zones has changed.	See "Configuration file updates" on page 169 for details of changes. To avoid problems in BIND 9 zones, you should use a $TTL directive in each zone file.	*z/OS Communications Server: IP Configuration Reference*

Table 123. IPv6 DNS for automatic rndc configuration for a local rndc client

Task	Procedure	Reference
Disable any existing rndc configuration.	Do the following: 1. Remove any control statements from named.conf. 2. Remove /etc/rndc.conf if it exists.	*z/OS Communications Server: IP Configuration Reference*
Create the /etc/rndc.key file.	Run rndc-confgen with the -a option	*z/OS Communications Server: IP System Administrator's Commands*
Allow the name server to read the /etc/rndc.key file and create the dynamic control channel for rndc.	Stop and restart the BIND9 name server.	*z/OS Communications Server: IP System Administrator's Commands*
Locally control the BIND9 name server.	Issue rndc commands to a local BIND9 name server.	*z/OS Communications Server: IP System Administrator's Commands*

Automatic rndc configuration for a local rndc client

In order to allow automatic configuration of a local rndc client for the BIND9 name server, perform the tasks in the following table.

Note: This will prevent remote rndc client control of the BIND9 name server.

Table 124. IPv6 DNS for automatic rndc configuration for a local rndc client

Task	Procedure	Reference
Disable any existing rndc configuration.	Do the following: 1. Remove any control statements from named.conf. 2. Remove /etc/rndc.conf if it exists.	*z/OS Communications Server: IP Configuration Reference*
Create the /etc/rndc.key file.	Run rndc-confgen with the -a option	*z/OS Communications Server: IP System Administrator's Commands*
Allow the name server to read the /etc/rndc.key file and create the dynamic control channel for rndc.	Stop and restart the BIND9 name server.	*z/OS Communications Server: IP System Administrator's Commands*
Locally control the BIND9 name server.	Issue rndc commands to a local BIND9 name server.	*z/OS Communications Server: IP System Administrator's Commands*

Part 3. SNA functions

Chapter 6. Roadmap to SNA functions

This chapter includes a table designed to be used as a roadmap to the SNA functions and enhancements that were introduced in z/OS V1R6 Communications ServerS, z/OS V1R5 Communications Server, and z/OS V1R4 Communications Server.

The **Enabling / migration actions** column indicates if tasks are required to either utilize the functional enhancement or to satisfy incompatibilities or dependencies. The **Reference** column points you to the section of this document that describes the function.

Table 125. Roadmap to SNA functions

Functional enhancement	Enabling / migration actions	Reference
Enhancements introduced in z/OS V1R6 Communications Server		
Display Enterprise Extender command enhancements	Yes	Page 179
Enterprise Extender Connection Network Reachability Awareness	No	Page 180
Support VARY ACT,UPDATE for Enterprise Extender XCA Major Nodes	Yes	Page 184
Allow V NET,INACT,ID=group and V NET,ACT,ID=group for Enterprise Extender GROUP	Yes	Page 185
VARY INACT,SCOPE=ALL support for Model APPLs	Yes	Page 186
Enhancements for multiple TRL major nodes	Yes	Page 186
SNA Enterprise Extender packet trace formatter	Yes	Page 187
IPINFO start option	Yes	Page 188
Display outstanding autologon requests	Yes	Page 188
CV64 IP address validity	Yes	Page 189
Display and message enhancements	No	Page 190
DUMP analysis enhancements for HPR	Yes	Page 192
DISPLAY RTPs by TCID	Yes	Page 192
EBN awareness of HPR sessions	Yes	Page 193
Enhanced addressing support for RTP PUs and DLUR PUs	No	Page 195
VARY TERM enhancements for APPN	Yes	Page 196
LSIRFMSG start option	Yes	Page 196
Persistent Session Forced Takeover	Yes	Page 198
Stalled HPR pipe recovery	Yes	Page 199
SNA/IP DISPLAY CSM enhancements	Yes	Page 200
Enhancements introduced in z/OS V1R5 Communications Server		
APPN trace enhancement	Yes	Page 203
CSDUMP command enhancements	Yes	Page 204
DLUR message enhancements	No	Page 205
Enterprise Extender enhancements	Yes	Page 205
RTP display enhancement	Yes	Page 213

Table 125. Roadmap to SNA functions (continued)

Functional enhancement	Enabling / migration actions	Reference
Session setup and problem determination enhancements	Yes	Page 213
Sift-down support for model major nodes	Yes	Page 215
Storage management enhancements	Yes	Page 215
Support for concurrent APING commands	Yes	Page 216
SWNORDER enhancements	Yes	Page 217
Trace performance enhancements	No	Page 218
HPR resequencing optimization	Yes	Page 219
MAXSLOW parameter for slowdown monitoring	Yes	Page 220
HPDT packing	Yes	Page 220
IPv6 support for SNA display of IP addresses	Yes	Page 221
CSM buffer tracking	Yes	Page 223
Improve diagnostics for DLC dumps	No	Page 224
OSA performance enhancements	Yes	Page 225
VTAM INOPDUMP enhancement	Yes	Page 225
IBM @server zSeries 990 HiperSockets enhancements	Yes	Page 228
Network management	Yes	Page 228
Enhancements introduced in z/OS V1R4 Communications Server		
CSALIMIT start option behavioral change	Yes	Page 231
Enterprise Extender dial processing enhancements	Yes	Page 232
Enterprise Extender addressing enhancement for logical lines and PUs	No	Page 233
Enable HPR-only VRNs for interchange sessions	Yes	Page 234
Display ID=rtpname diagnostic enhancement	Yes	Page 235
SRB mode dump enhancement	No	Page 236
Increase maximum value for AUTOGEN on XCA major nodes	Yes	Page 236
VIT data timestamp enhancement	Yes	Page 237
VARY ACT,UPDATE command for CDRSC Major Nodes enhancement	Yes	Page 238
OPEN Application Control Block (ACB) limit increase	No	Page 239
NQNMODE support for Directory Services (DS) database entries	Yes	Page 240
Changes to installing dump analysis and trace analysis tools	No	Page 241
APPN topology traces enhancements	No	Page 242
VTAM IPCS CLIST changes	No	Page 243
VTAM INOPDUMP enhancement	Yes	Page 244
New start options to adjust the QDIO or iQDIO storage	Yes	Page 245

Chapter 7. V1R6 SNA new function summary

This chapter includes a section for every function or enhancement introduced for SNA in z/OS V1R6 Communications Server. The sections include the following 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.

See Table 125 on page 177 for a complete list of the SNA functional enhancements of the current and recent releases.

Refer to *z/OS Migration* for information about how to maintain the functional behavior of previous releases. Refer to *z/OS Summary of Message and Interface Changes* for information on new and changed messages and interfaces.

Display Enterprise Extender command enhancements

Enterprise Extender is IBM's strategic SNA/IP integration and migration protocol. There are a number of network management tools available for monitoring and problem diagnosis with TCP/IP and SNA. Until z/OS V1R6 Communications Server, however, no existing operator commands provided access to Enterprise Extender specific network management and problem diagnosis information.

In z/OS V1R6 Communications Server, a new VTAM display command, DISPLAY EE, helps to better manage Enterprise Extender networks. Various formats of the new display give the operator the ability to obtain general Enterprise Extender information, as well as connection specific information, including transmission statistics broken down by port priority.

Restrictions

None.

What this change affects

- Diagnosis
- Operations

Using this function

The Display Enterprise Extender command enhancements do not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Refer to DISPLAY EE command and DISPLAY RTPS command in *z/OS Communications Server: SNA Operation* as you complete the tasks.

Table 126. Display Enterprise Extender command

Task	Procedure
Display the total number of active Enterprise Extender connections.	Issue the DISPLAY EE command.
Display the total number of RTP pipes and LU-LU sessions using Enterprise Extender.	Issue the DISPLAY EE command.
Display the number of available dial-in lines associated with a specific EE VRN.	Issue the DISPLAY EE,LIST=DETAIL command.
Display the number of RTP pipes and LU-LU sessions associated with a specific EE switched PU.	Issue the DISPLAY EE,ID=*puname* command.
Obtain a list of RTP pipes traversing a specific EE switched PU.	Issue DISPLAY RTPS,ALSNAME=*name* command.
If poor response time is being reported to a specific remote EE endpoint, display the total number of retransmitted NLPs, broken down by transmission priority, to that remote EE endpoint.	Issue one of the following commands: • DISPLAY EE,ID=*linename*,DET • DISPLAY EE,ID=*puname*,DET • DISPLAY EE,HN=(,remote_hostname),DET • DISPLAY EE,IP=(,remote_IPADDR),DET
Obtain the total number of bytes, by transmission priority, that have been transmitted to a specific EE partner.	Issue one of the following commands: • DISPLAY EE,ID=*linename*,DET • DISPLAY EE,ID=*puname*,DET • DISPLAY EE,HN=(,remote_hostname),DET • DISPLAY EE,IP=(,remote_IPADDR),DET
Obtain aggregate throughput totals for all EE connections associated with a remote hostname (IPv6).	Issue the DISPLAY EE,HN=(,remote_hostname) command.
Obtain aggregate statistics for all active EE connections associated with a local_hostname or a local_IPADDR.	Issue one of the following commands: • DISPLAY EE,ID=local_hostname • DISPLAY EE,ID=local_IPADDR

Enterprise Extender Connection Network Reachability Awareness

This function provides improved availability for sessions using Enterprise Extender connection networks by selecting an available alternate path for session routes when connectivity fails over an EE connection network. A new start option, UNRCHTIM, is provided to control how long VTAM waits after an EE connection network failure before the EE connection network is retried, thus allowing time for the connectivity problem to be corrected. UNRCHTIM can also be coded on a PORT or GROUP definition statement that defines a connection network in an Enterprise Extender External Communications Adapter (XCA) major node, which allows a specific connection network to have a different unreachable time value than the value specified on the UNRCHTIM start option.

It is important to understand the ramifications of the UNRCHTIM value you choose. The results can vary depending on the duration of failures that occur. A value that is appropriate for a short term failure might not be appropriate for a long term failure. You should review the considerations of this function in the UNRCHTIM considerations section in *z/OS Communications Server: SNA Network Implementation Guide* prior to implementation.

If you are currently using automation with message IST1903I (added in z/OS V1R5 Communications Server) to deal with this problem, you should remove this

automation if you decide to implement the EE Connection Network Reachability Awareness function and allow automatic routing around Enterprise Extender connection network problems.

In addition, a new LIST option for the DISPLAY TOPO command, LIST=UNRCHTIM, allows you to display unreachable paths across Enterprise Extender connection networks. It also displays the time the unreachable time expires for each unreachable path.

This function also introduces a new FUNCTION option for the MODIFY TOPO command, FUNCTION=CLRUNRCH. It allows you to clear unreachable partner information for an Enterprise Extender virtual node or an end node that is the origin of unreachable paths through Enterprise Extender virtual nodes.

Refer to the EE connection network reachability awareness section in *z/OS Communications Server: SNA Network Implementation Guide* for further details of this function.

Restrictions

The Enterprise Extender Connection Network Reachability Awareness function is restricted to Enterprise Extender connection networks.

Coexistence requirements

A complete implementation of this function requires that all z/OS Communications Server network nodes, and all z/OS Communications Server end nodes that connect to Enterprise Extender virtual nodes, be running z/OS V1R6 or higher. However, even if some of these nodes are not running z/OS V1R6 or higher, this function can still be exploited for some sessions if the following nodes are both running z/OS V1R6 or higher:

- The network node or end node on the origin (primary LU) side of the VRN
- The network node responsible for computing the session path

What this change affects

- Diagnosis
- Availability
- Operations
- Usability

Using this function

The Enterprise Extender Connection Network Reachability Awareness function can be turned on with a new UNRCHTIM start option, or a new UNRCHTIM keyword on an Enterprise Extender External Communications Adapter (XCA) GROUP or PORT definition statement. Refer to the tasks in the following table for details.

Table 127. Enterprise Extender Connection Network Reachability Awareness

Task	Procedure	Reference
Set the default unreachable time for all Enterprise Extender connection networks.	Set the UNRCHTIM start option to a non-zero value in the VTAM start list, ATCSTRxx.	UNRCHTIM in *z/OS Communications Server: SNA Resource Definition Reference*

Table 127. Enterprise Extender Connection Network Reachability Awareness (continued)

Task	Procedure	Reference
Change the default unreachable time for all Enterprise Extender connection networks.	Issue MODIFY VTAMOPTS,UNRCHTIM=*time* command, with *time* as the number of seconds the path remains unreachable.	MODIFY VTAMOPTS command in *z/OS Communications Server: SNA Operation* and UNRCHTIM in *z/OS Communications Server: SNA Resource Definition Reference*
If the unreachable time start option is set to a non-zero value, turn OFF (by default) the unreachable path function.	Issue MODIFY VTAMOPTS,UNRCHTIM=0 command.	MODIFY VTAMOPTS command in *z/OS Communications Server: SNA Operation* and UNRCHTIM in *z/OS Communications Server: SNA Resource Definition Reference*
Set an unreachable time for a specific Enterprise Extender connection network.	Specify UNRCHTIM=*time* on the PORT or GROUP definition statement which has VNNAME or VNTYPE coded in an Enterprise Extender XCA major node, with *time* as the number of seconds the path remains unreachable. Then issue VARY ACT,ID=majnode if the major node has not previously been activated, or VARY ACT,ID=majnode,UPDATE=ALL if the major node is already active.	UNRCHTIM in *z/OS Communications Server: SNA Resource Definition Reference*
If the unreachable time start option is set to a non-zero value or the unreachable time is non-zero on the PORT or GROUP definition statement which has VNNAME or VNTYPE coded in an Enterprise Extender XCA major node, turn OFF the unreachable path function for that specific Enterprise Extender connection network.	Specify UNRCHTIM=0 on the PORT or GROUP definition statement which has VNNAME or VNTYPE coded in an Enterprise Extender XCA major node. Then issue VARY ACT,ID=majnode if the major node has not previously been activated, or VARY ACT,ID=majnode,UPDATE=ALL if the major node is already active.	UNRCHTIM in *z/OS Communications Server: SNA Resource Definition Reference*
Display all unreachable Enterprise Extender connection network paths known in this node.	Issue DISPLAY TOPO,LIST=UNRCHTIM command.	DISPLAY TOPO command in *z/OS Communications Server: SNA Operation*, Displaying unreachable partner information in *z/OS Communications Server: SNA Network Implementation Guide*, and Display Enterprise Extender connection network unreachable partner information in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*

Table 127. Enterprise Extender Connection Network Reachability Awareness (continued)

Task	Procedure	Reference
Display all unreachable Enterprise Extender connection network paths associated with a specific VRN.	Issue DISPLAY TOPO,LIST=UNRCHTIM,ID=vrn_cp_name.	DISPLAY TOPO command in *z/OS Communications Server: SNA Operation*, Displaying unreachable partner information in *z/OS Communications Server: SNA Network Implementation Guide*, and Display Enterprise Extender connection network unreachable partner information in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*
Display unreachable Enterprise Extender connection network paths associated with a specific origin EN.	Issue DISPLAY TOPO,LIST=UNRCHTIM,ID=en_cp_name.	DISPLAY TOPO command in *z/OS Communications Server: SNA Operation*, Displaying unreachable partner information in *z/OS Communications Server: SNA Network Implementation Guide*, and Display Enterprise Extender connection network unreachable partner information in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*
Clear all unreachable partner information associated with a specific origin EN.	Issue MODIFY TOPO,FUNCTION=CLRUNRCH,SCOPE= NETWORK,ID=en_cp_name command on the EN.	MODIFY TOPO command in *z/OS Communications Server: SNA Operation*, Clearing unreachable partner information in *z/OS Communications Server: SNA Network Implementation Guide*, and Modify TOPO to clear EE connection network unreachable partner information in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*
Clear all unreachable partner information associated with a specific Enterprise Extender VRN on one network node.	Issue MODIFY TOPO,FUNCTION=CLRUNRCH,ID= vrn_cp_name or F TOPO,FUNCTION=CLRUNRCH,SCOPE= LOCAL,ID=vrn_cp_name command on the NN.	MODIFY TOPO command in *z/OS Communications Server: SNA Operation*, Clearing unreachable partner information in *z/OS Communications Server: SNA Network Implementation Guide*, and Modify TOPO to clear EE connection network unreachable partner information in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*

Table 127. Enterprise Extender Connection Network Reachability Awareness (continued)

Task	Procedure	Reference
Clear all unreachable partner information associated with a specific Enterprise Extender VRN on all network nodes in the network.	Issue MODIFY TOPO,FUNCTION=CLRUNRCH,SCOPE=NETWORK,ID=vrn_cp_name command on any NN in the network.	MODIFY TOPO command in *z/OS Communications Server: SNA Operation*, Clearing unreachable partner information in *z/OS Communications Server: SNA Network Implementation Guide*, and Modify TOPO to clear EE connection network unreachable partner information in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*

VARY command enhancements for Enterprise Extender and TRL and Model APPLs

The following sections describe the VARY command enhancements:

- "Support VARY ACT,UPDATE for Enterprise Extender XCA Major Nodes"
- "Allow V NET,INACT,ID=group and V NET,ACT,ID=group for Enterprise Extender GROUP" on page 185
- "VARY INACT,SCOPE=ALL support for Model APPLs" on page 186
- "Enhancements for multiple TRL major nodes" on page 186

Support VARY ACT,UPDATE for Enterprise Extender XCA Major Nodes

This function provides the ability to make modifications to the Enterprise Extender XCA major node definitions without inactivating the major node. This allows configuration changes to be made at the GROUP level or lower while other Enterprise Extender connections remain active. This function also makes it possible to make changes to operands for virtual node definitions on the PORT statement as long as the GROUP named by VNGROUP is inactive. This enables configuration changes to be made with less disruption to users.

Restrictions

Definition changes to an Enterprise Extender GROUP definition, adding a LINE, or deleting a LINE will require the GROUP and all subordinate resources to be inactive. Definition changes to an Enterprise Extender LINE definition will require the LINE to be inactive. Supported changes of virtual node values on the PORT will require that the GROUP named by VNGROUP be inactive.

This function is only supported for the Enterprise Extender XCA major node.

What this change affects

- Availability
- Operations
- Usability

Using this function

This function does not require any action unless you want to take advantage of it. If so, perform the desired tasks in the following table.

Refer to the VARY INACT command and the VARY ACT command in *z/OS Communications Server: SNA Operation* for more information.

Table 128. Support VARY ACT,UPDATE for Enterprise Extender XCA Major Nodes

Task	Procedure
Make modifications to the Enterprise Extender XCA major node definitions: • Add a LINE to an Enterprise Extender GROUP. • Add a GROUP to an Enterprise Extender major node. • Delete a LINE from an Enterprise Extender GROUP. • Delete a GROUP from an Enterprise Extender major node. • Modify a GROUP parameter.	Issue VARY INACT ID=groupname,SCOPE=ALL to inactivate the GROUP and all subordinate LINES. Edit the Enterprise Extender XCA major node member in VTAMLST. Issue VARY ACT ID=majornode,UPDATE=ALL to enable the definition change.
Modify a LINE parameter.	Issue VARY INACT,ID=linename to inactivate the LINE. Edit the Enterprise Extender XCA major node member in VTAMLST. Issue VARY ACT,ID=majornode,UPDATE=ALL to enable the definition change.
Modify PORT connection network values.	Issue VARY INACT,ID=groupname for the GROUP named by VNGROUP. Edit the Enterprise Extender XCA major node member in VTAMLST. Issue VARY,ACT,ID=majornode,UPDATE=ALL to enable the definition change.

Allow V NET,INACT,ID=group and V NET,ACT,ID=group for Enterprise Extender GROUP

This function improves usability by providing the ability to activate and deactivate an entire group (including all of the lines under the group) of an Enterprise Extender XCA major node with a single command. This function may be helpful to those using the VARY ACT,UPDATE enhancement.

Restrictions

This function only works for GROUPs in the Enterprise Extender XCA major node; other GROUPs are not supported for this function.

What this change affects

- Availability
- Operations
- Usability

Using this function

This function does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Refer to the VARY INACT command and the VARY ACT command in *z/OS Communications Server: SNA Operation* for more information.

Table 129. Allow V NET,INACT,ID=group and V NET,ACT,ID=group for Enterprise Extender GROUP

Task	Procedure
Activate or deactivate Enterprise Extender Group.	Issue VARY ACT/INACT ID=group_name to activate or deactivate the group.
Activate Group and all the Lines under the Enterprise Extender GROUP.	Issue VARY ACT ID=group_name,SCOPE=ALL to activate the group and all of the lines under it.

VARY INACT,SCOPE=ALL support for Model APPLs

This enhancement provides improved availability and usability in the support of Model APPLs. Specifically, it simplifies processing by providing the ability to deactivate a Model APPL and all of the APPL Clones generated from the specified Model APPL with one simple command.

Restrictions

None.

What this change affects

- Availability
- Operations
- Usability

Using this function

This function does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 130. VARY INACT,SCOPE=ALL support for Model APPLs

Task	Procedure	Reference
Deactivate Model APPL and all of the APPLs generated from the specified model.	Issue VARY INACT ID=model_appl_name,SCOPE=ALL to deactivate the model APPL and all of the APPLs generated from the specified model.	VARY INACT command in *z/OS Communications Server: SNA Operation*

Enhancements for multiple TRL major nodes

This enhancement provides improved availability and usability in the support of TRL major nodes. Prior to this change, ISTTRL included both predefined and dynamic TRLEs. The ISTTRL major node will only include dynamically defined TRLEs. To create predefined TRLEs, TRL major nodes may now be defined, activated, updated, and inactivated like any other major node. The TRL major nodes may also be displayed.

Restrictions

None.

What this change affects

- Availability
- Operations
- Usability

Using this function

This function does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Refer to the DISPLAY TRL command in *z/OS Communications Server: SNA Operation* for more information.

Table 131. Enhancements for Multiple TRL Major Nodes

Task	Procedure
Display a predefined TRL major node.	Issue DISPLAY TRL,TRLMN=trl_major_node_name to display an active TRL major node.
Display only the dynamically defined TRLEs.	Issue one of the following commands: • DISPLAY NET,TRL,TRLMN=ISTTRL • DISPLAY NET,ID=ISTTRL,E

SNA Enterprise Extender packet trace formatter

z/OS V1R6 Communications Server enhances the formatting of TCP/IP packet traces to include Enterprise Extender packets that flow to and from TCP/IP. Prior to z/OS V1R6 Communications Server, Enterprise Extender packets could only be dumped.

Note: In z/OS V1R6 Communications Server, the SYSTCPDA record type 6 is new for Enterprise Extender. Types 1, 2, and 3 are discontinued.

Restrictions

None.

Dependencies

TCP/IP must be installed.

What this change affects

- Diagnosis

Using this function

If you want to use the Enterprise Extender packet trace formatter, perform the tasks in the following table.

Table 132. SNA Enterprise Extender packet trace formatter

Task	Procedure	Reference
Start packet traces.	Issue VARY TCPIP,,PKTTRACE,DESTP=12000 and VARY TCPIP,,PKTTRACE,SRCP=12000. Repeat for ports 12001 through 12004.	VARY TCPIP,,PKTTRACE in *z/OS Communications Server: IP System Administrator's Commands*
Format packet traces.	Issue the following command using IPCS: CTRACE COMP(SYSTCPDA) OPTIONS((EE FORMAT)).	Packet trace (SYSTCPDA) for TCP/IP stacks in *z/OS Communications Server: IP Diagnosis Guide*

IPINFO start option

By default, when VTAM receives TCP/IP information from a TN3270 server in the TCP/IP Information Control Vector CV X'64', it exposes the information through all supported interfaces, such as displays, exits, and in cross-domain flows to other nodes. z/OS V1R6 introduces a new IPINFO start option that controls how VTAM exposes this TCP/IP information.

Tip: The IPINFO start option has no effect on whether VTAM will forward TCP/IP information received from other hosts when acting as an intermediate node on the path of session establishment requests. As an intermediate node, VTAM will pass through TCP/IP information in the same way it would pass through other unrecognized information.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Security
- Usability

Using this function

The IPINFO start option enhancement does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 133. IPINFO start option enhancement

Task	Procedure	Reference
Control the saving and distribution of TCP/IP characteristics for TN3270 clients.	Code the IPINFO start option with an appropriate value. Use the MODIFY VTAMOPTS command to change the IPINFO start option to an appropriate value.	IPINFO in *z/OS Communications Server: SNA Resource Definition Reference* and MODIFY VTAMOPTS command in*z/OS Communications Server: SNA Operation*

Display outstanding autologon requests

Coding LOGAPPL= on an LU resource drives a session attempt when the LU becomes session capable. If the session fails, an outstanding autologon request is created in the LU host. Outstanding autologon requests are periodically driven by the setting of the AUTOTI and AUTORTRY start options. A DSRLST is sent into the network to search for the controlling application. If LOGAPPL= is coded with an incorrect name, or the controlling application no longer exists, or the path to the application no longer exists, the attempts to locate the application will send unneeded searches into the network.

A new DISPLAY AUTOLOG command allows for the display of names of controlling applications for which there are outstanding autologon requests. The command also displays the conditions that would cause these pending autologon requests to be initiated again, and optionally lists the names of secondary logical

units that have autologon requests pending for each controlling application that is displayed. This command can provide awareness of pending autologon activity.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

The display outstanding autologon requests function does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Refer to DISPLAY AUTOLOG command in *z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages* for more information.

Table 134. Display outstanding autologon requests

Task	Procedure
Display a list of controlling applications that have pending autologon requests.	Issue the DISPLAY NET,AUTOLOG command.
Display a list of controlling applications that have lost their controlling sessions to one or more LUs and the LUs that are waiting for each.	Issue the DISPLAY NET,AUTOLOG,SCOPE=ALL command.
Display a specific controlling application that has a pending autologon request.	Issue the DISPLAY NET,AUTOLOG,ID= controlling_application_name command.
Display a specific controlling application that has lost a controlling session to one or more LUs.	Issue the DISPLAY NET,AUTOLOG,ID= controlling_application_name commands. It will include a list of LUs that are waiting for the controlling application.

CV64 IP address validity

The z/OS Communications Server TN3270 server can configure the TKOSPECLURECON or TKOGENLURECON profile parameter for session recovery. As part of the recovery, it is possible that when the TN3270 client reconnects, it could have a different IP address than the one prior to the disconnect. This can cause some inconsistencies with VTAM functions that associate the TN3270 client IP address with the LU name. In this case, the TN3270 server still has the same LU but the IP address associated with the LU has changed. When this occurs, exits and cross-domain hosts that received the original IP address will not be updated with the new IP address; however, the local VTAM will display the new IP address.

To address this problem, an indicator in the TCP/IP Control Information Vector CV X'64' has been added to alert hosts and applications that process the CV X'64' that the TKOSPECLURECON or TKOGENLURECON is specified by the TN3270 server, allowing exits that process this information to make decisions on how to handle this situation.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Security
- Usability

Using this function

The CV64 IP address validity enhancement does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 135. CV64 IP address validity

Task	Procedure	Reference
Determine if the IP address associated with TN3270 server session is subject to change due to the TN3270 configuration parameter TKOSPECLURECON or TKOGENLURECON.	Interrogate new CV64 indicator field from PLU application during LOGON exit processing.	*SNA Formats*

Display and message enhancements

z/OS V1R6 Communications Server introduces the following enhancements to improve serviceability and increase network awareness:

- **New information is added to the SNA display command output for selected resources.**
  - Additional information is now provided on SNA displays for certain types of PUs while they are active:
    - Route Information Field (RIF) data, when available, will appear on displays of PUs with type 2.1 LAN connections.
    - IDBLK and IDNUM will appear on displays of PUs with type1 or type2 connections.
  - The LOCADDR value is now provided on SNA displays for Logical Units.
  - You can now determine whether or not a given SNA application is APPC-capable simply by looking at a SNA display of the application. The value of the APPC parameter (YES|NO) specified or defaulted on the APPL definition statement will be indicated in the message group that appears whenever a DISPLAY NET,ID= command for the SNA application is issued.
  - You can now easily determine if a VARY INACT command with FINAL=YES specified has been issued against a particular DLUR. This new information (FINAL=YES|NO) will now appear in the display output of a DISPLAY NET,ID= command for the DLUR CDRSC.
- **Additional information is now provided on all SNA displays for Rapid Transit Protocol (RTP) PUs.**
  - The transmission priority of the APPN Class of Service being used.
  - The time the RTP pipe was activated and the role of the PU (active or passive).

- **SNA displays for Rapid Transit Protocol (RTP) PUs when HPRDIAG=YES is specified on the corresponding DISPLAY NET,ID= command have been reorganized.**

  The following new information has been added as well:
  - High water mark for the actual data flow rate
  - Rate reductions due to retransmissions
  - The Short Request Timer value
  - Sequence number of the last packet sent
  - The total number of bytes sent
  - The total number of bytes retransmitted
  - Maximum number of NLPs on the waiting-for-acknowledgement queue and the time when maximum was reached
  - Sequence number of the last packet received
  - The total number of bytes received
  - Number of NLPs currently on the inbound work queue
  - Maximum number of NLPs on the inbound work queue
  - Number of RTP path switches initiated from remote partner
  - Number of RTP path switches initiated locally
  - Number of RTP path switches due to local failure
  - Number of RTP path switches due to local PSRETRY
- **Additional information is provided for HPR path switching events.**
  - SNA messages currently issued for some HPR Path Switches give no indication of the location of the other end of the RTP pipe. To enhance notification of locally triggered path switches, the CP name of the node at the remote end of the RTP pipe is now appended to message IST1494I. This should adequately identify the remote partner, whether the path switch was a failure or a success.
  - For remotely triggered path switches, a new message will appear to indicate the reason for the path switch. Completion will be indicated by IST1494I. If the RTP PU is subsequently displayed (specifying HPRDIAG=YES), the new message will appear as the reason for the most recent path switch.
- **Unsolicited information about HPR path switches is now routed to the Primary Program Operator (PPO) instead of the operator console.**

  SNA messages related to HPR path switching events had been automatically directed to the operator console, so they would appear in VTAM joblog as well as the syslog. Such messages are now directed to the selected PPO only, except when a path switch is due to an operator-initiated MODIFY RTP command.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

There are no specific tasks associated with the SNA display and message enhancements.

DUMP analysis enhancements for HPR

A new IPCS VTAMMAP command option, RTPINFO, is provided for the analysis of dumps taken for High Performance Routing (HPR) problems. VTAMMAP RTPINFO will gather and display information about HPR RTPs from the dump. This will greatly improve the diagnosis of HPR problems.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

The DUMP analysis enhancements for HPR do not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 136. DUMP analysis enhancements for HPR

Task	Procedure	Reference
Display information about RTP pipes in a dump.	From IPCS, issue the following command: VERBX VTAMMAP 'RTPINFO'	RTPINFO in *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*

DISPLAY RTPs by TCID

This function enhances the DISPLAY RTPS command to allow an RTP to be displayed by specifying only the local Transport Connection Identifier (TCID) for the RTP. This new variation of the DISPLAY RTPS command can be used to correlate a local RTP PU name to the RTP PU name used by the remote VTAM partner RTP node to represent the same RTP connection.

To determine the RTP PU name used by the remote VTAM partner RTP node, use the DISPLAY ID=rtp_pu_name command on the local node to display the RTP PU and remember the REMOTE TCID value that is displayed on the end of the IST1476I message. Then, from the remote VTAM partner RTP node (shown on the IST1481I message in the prior display), issue the DISPLAY RTPS,TCID=tcid_value command using the REMOTE TCID value obtained from the prior display.

Restrictions

Because TCIDs are only guaranteed to be unique within the node that defines them, this command allows only the local TCID to be specified using the new TCID operand.

What this change affects

- Operations

Using this function

The DISPLAY RTPs by TCID enhancement does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Refer to DISPLAY RTPS command in *z/OS Communications Server: SNA Operation* for more information.

Table 137. DISPLAY RTPs by TCID

Task	Procedure
Display an RTP PU using the local TCID.	Issue the DISPLAY RTPS,TCID= command.
Given the name of a local RTP PU, determine the RTP PU name used by the remote VTAM partner RTP node to represent the same RTP connection.	From the local host, issue the DISPLAY ID=rtp_pu_name command and remember the REMOTE TCID value displayed on the IST1476I message. Then, from the remote VTAM partner RTP node (identified by the IST1481I message in the output of the previous command), issue the DISPLAY RTPS,TCID= command specifying the REMOTE TCID obtained from the previous command.

EBN awareness of HPR sessions

The use of HPR for sessions that cross APPN subnetwork boundaries can prevent the border nodes along the session path from maintaining awareness of these sessions. (If a border node on the session path is performing only the ANR function for these sessions, then no session awareness is maintained.)

This function addresses this situation by improving your ability to monitor sessions that are established into or through your APPN network. It allows customers who configure border nodes within their network to specify through which adjacent nonnative nodes should new RTPs be allowed to be established without maintaining session awareness.

This function is enabled by coding the new RTPONLY operand on adjacent CP (ADJCP) definitions.

Restrictions

The following restrictions apply:

- RTPONLY can only be specified on ADJCP definitions that are activated on border nodes (BN=YES). The RTPONLY operand is ignored and an error message is issued if the activating node is not a border node.
- RTPONLY=YES requires that RTP be specified as the first operand of the HPR start option. RTPONLY=YES is ignored and an error message is issued if the activating node has not specified HPR=RTP or HPR=(RTP,RTP|ANR|NONE).
- RTPONLY=YES is only meaningful on ADJCP definitions that represent nonnative nodes (that is, network nodes or border nodes that are not part of the local APPN subnetwork). As a result, RTPONLY=YES is not allowed with NATIVE=YES, NN=NO or VN=YES. The RTPONLY operand is ignored for any ADJCP definition that represents a native network node or end node.
- Use of RTPONLY=YES at any APPN subnetwork boundary on a session setup path will prevent the use of Global VRNs (GVRNs) for intersubnetwork connectivity, since using GVRNs could result in sessions being established across this subnetwork boundary without this border node maintaining awareness of these sessions.
- Use of RTPONLY=YES can result in an increase in network traffic in the form of additional Route_Setup flows used for RTP establishment. These additional Route_Setup flows will only occur during the establishment of sessions that cross subnetwork boundaries defined with RTPONLY=YES.

- Use of RTPONLY=YES can result in an increase in storage and CPU utilization due to VTAM maintaining awareness of these sessions and performing ISR instead of HPR/ANR for these sessions.
- An RTP that is established over a path with RTPONLY=NO specified will not be allowed to path switch to an alternate path that has RTPONLY=YES specified. Therefore, defining alternate paths to the same destination APPN subnetwork with differing values for RTPONLY may result in path switch processing failing to find a viable alternate path during an outage. This could happen during the initial deployment of this function while some border nodes have RTPONLY=YES enabled and others have not, or as a result of forgetting to enable this function at some of the subnetwork boundaries that provide alternate paths to the same nonnative subnetwork.

What this change affects

- Diagnosis
- Availability
- Operations
- Performance
- Security
- Storage
- Usability

Using this function

The EBN awareness of HPR sessions does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Table 138. EBN awareness of HPR sessions

Task	Procedure	Reference
On a border node, define an adjacent nonnative node through which ANR routing should ***not*** be allowed.	Define the adjacent nonnative node in an ADJCP major node (VBUILD TYPE=ADJCP) and include RTPONLY=YES on the minor node definition for the adjacent nonnative node.	Adjacent control point major node in *z/OS Communications Server: SNA Resource Definition Reference*
On a border node, define an adjacent nonnative node through which ANR routing should be allowed.	Define the adjacent nonnative node in an ADJCP major node (VBUILD TYPE=ADJCP) and include RTPONLY=NO on the minor node definition for the adjacent nonnative node. Alternatively, you can omit the RTPONLY operand; or you can avoid defining this adjacent nonnative node completely (assuming DYNADJCP=YES is specified). In either case, RTPONLY=NO will be used by default.	Adjacent control point major node in *z/OS Communications Server: SNA Resource Definition Reference*

Table 138. EBN awareness of HPR sessions (continued)

Task	Procedure	Reference
On a border node, nondisruptively modify the RTPONLY value associated with an adjacent nonnative node.	If an ADJCP definition for the adjacent nonnative node to be changed has already been activated, then the entire ADJCP major node containing that definition must first be inactivated using the VARY INACT,ID=adjcp_major_node command. **Note:** Inactivating a predefined ADJCP major node does not cause links or CP-CP sessions to be terminated. Rather, the adjacent CP definitions for nodes that currently have active connections to this node are preserved by moving them to the dynamic ADJCP major node, ISTADJCP. During this process, the current RTPONLY value in effect will be preserved. After creating or modifying the necessary ADJCP definitions, activate (or reactivate) the ADJCP major node using the VARY ACT,ID=adjcp_major_node command.	Adjacent control point major node in *z/OS Communications Server: SNA Resource Definition Reference*, and the VARY INACT command and the VARY ACT command in *z/OS Communications Server: SNA Operation*
On a border node, display the RTPONLY value associated with an adjacent nonnative node.	Issue the DISPLAY ADJCP,ID=adjcpname,SCOPE=ALL command. Alternatively, if there is at least one RTP connection from this node to the adjacent nonnative node, then you can also issue the DISPLAY ID=adjcp_major_node,SCOPE=ALL command.	DISPLAY ADJCP command in *z/OS Communications Server: SNA Operation*

Enhanced addressing support for RTP PUs and DLUR PUs

Enhanced addressing support for RTP PUs and DLUR PUs removes the constraint of network addresses for HPR and DLUR PUs by expanding the network address allocations, above and beyond the 64K line, up to 33M. This allows the limited number of low-order element addresses to be used for other things and allows for network growth for the number of HPR pipes and DLUR PUs that may be required in an Enterprise Extender environment by assigning extended (high-order) element addresses to RTP PUs and DLUR PUs.

Restrictions

The highest number of element addresses that can be assigned for RTP PUs and DLUR PUs is now 33M.

What this change affects

- Performance
- Availability
- Operations
- Usability

Using this function

There are no tasks required to use the enhanced addressing support for RTP PUs and DLUR PUs ; it is automatically enabled.

VARY TERM enhancements for APPN

In rare cases, an APPN search for a session resource may not produce a response. If an APPN search remains hung without a response, future search requests for the same resource will wait for the first search request to complete. To allow a hung APPN search request to be cleaned up, a new option on the VARY TERM command, SCOPE=APPN, is provided to force termination of the search request. This function can be used to clean up hung APPN search requests that cannot be terminated by using another flavor of the VARY TERM command. This new function will enhance the availability of SNA network resources by allowing future search requests to complete.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

The VARY TERM enhancements for APPN do not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Table 139. VARY TERM enhancements for APPN

Task	Procedure	Reference
Determine SID for search request.	Issue DISPLAY NET,SRCHINFO,LIST=ALL.	DISPLAY SRCHINFO command in *z/OS Communications Server: SNA Operation*
Terminate APPN search request.	Issue VARY TERM,SCOPE=APPN,SID=sid_value.	VARY TERM command in *z/OS Communications Server: SNA Operation*

LSIRFMSG start option

A new VTAM start option is introduced to provide additional information to help diagnose the reason for APPN locate search failures using the IST663I message group.

Setting LSIRFMSG and ESIRFMSG will result in the IST891I message group being issued for APPN locates. Setting LSIRFMSG and FSIRFMSG will result in a new message group being issued to display results of all APPN locate search steps. These messages provide detailed information to help determine why the APPN locate failed to find a network resource.

Coding SIRFMSG= and CPNAME= on CDRSC definitions will now also affect LSIRFMSG processing. Therefore, you may see an increase in the number of messages that are displayed for resources that you currently have defined with these operands.

Coding SIRFMSG= on APPL definitions has no effect on LSIRFMSG processing.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Usability

Using this function

You are not required to use the new LSIRFMSG start option. If you choose to use it, perform the desired tasks in the following table.

Table 140. LSIRFMSG start option

Task	Procedure	Reference
Enable APPN locate search messages for diagnosis at VTAM startup.	Code start option LSIRFMSG on a Network Node. LSIRFMSG=ALLNNS will result in failure messages being issued for searches where this node is acting as a network node. LSIRFMSG=OLUNNS will result in failure messages being issued for searches where this node is acting as a network node server of the OLU. **Tip:** When the LSIRFMSG start option is enabled, the ESIRFMSG and FSIRFMSG start options can be used to provide more detailed information on why an APPN search failed. If more detailed information is desired, then consider enabling these start options as well: • MODIFY NET,VTAMOPTS,ESIRFMSG=ALLSSCP, FSIRFMSG=ALLSSCP • MODIFY NET,VTAMOPTS,ESIRFMSG=OLUSSCP, FSIRFMSG=OLUSSCP	LSIRFMSG in *z/OS Communications Server: SNA Resource Definition Reference*
Enable APPN locate search messages for diagnosis after VTAM startup.	Modify start option LSIRFMSG on a Network Node by issuing the following commands: • MODIFY NET,VTAMOPTS,LSIRFMSG=ALLNNS • MODIFY NET,VTAMOPTS,LSIRFMSG=OLUNNS **Tip:** When the LSIRFMSG start option is enabled, the ESIRFMSG and FSIRFMSG start options can be used to provide more detailed information on why an APPN search failed. If more detailed information is desired, then consider enabling these start options as well. • MODIFY NET,VTAMOPTS,ESIRFMSG=ALLSSCP, FSIRFMSG=ALLSSCP • MODIFY NET,VTAMOPTS,ESIRFMSG=OLUSSCP, FSIRFMSG=OLUSSCP	LSIRFMSG in *z/OS Communications Server: SNA Resource Definition Reference*
Disable APPN locate search messages after diagnostic information has been collected.	Modify start option LSIRFMSG on a Network Node by issuing the following commands: • MODIFY NET,VTAMOPTS,LSIRFMSG=NONE • MODIFY NET,VTAMOPTS,LSIRFMSG=NONE	MODIFY VTAMOPTS command in *z/OS Communications Server: SNA Operation*

Table 140. LSIRFMSG start option (continued)

Task	Procedure	Reference
Display APPN locate search messages start option value.	Display start option LSIRFMSG on a Network Node by issuing the following commands: • DISPLAY NET,VTAMOPTS,OPT=LSIRFMSG • DISPLAY NET,VTAMOPTS,OPT=LSIRFMSG	DISPLAY VTAMOPTS command in *z/OS Communications Server: SNA Operation*
Enable or disable APPN locate search failure messages for a single cross domain resource.	Code SIRFMSG= and CPNAME= on the CDRSC definition.	CDRSC definition statement in *z/OS Communications Server: SNA Resource Definition Reference*

Persistent Session Forced Takeover

Prior to z/OS V1R6, MNPS takeover processing required a level of prior coordination between the taking over application and the existing application; in particular, that the existing application must first issue a CLOSE ACB while enabled for persistence. There are cases where you might want to initiate MNPS takeover without first waiting for the application being taken over to get into the proper recovery state. That capability is now provided by MNPS Forced Takeover processing if the application indicates that it will support it.

In conjunction with this change, a persistent capable application may now indicate that SNPS takeover requests should not be accepted. Previously, the application had no way to prevent being taken over, while still active, as part of SNPS processing.

Restrictions

The nodes that own the application issuing the forced MNPS takeover request and the application being taken over must be at least z/OS V1R6 or higher.

Dependencies

The application must be programmed to exploit this function.

What this change affects

- Application development
- Availability
- Performance
- Usability

Using this function

The enhancements for Persistent Session Forced Takeover do not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Refer to the Application program recovery with multinode persistence enabled section in *z/OS Communications Server: SNA Programming* for more information.

Table 141. Enhancements for Persistent Session Forced Takeover

Task	Procedure
Indicate that this application supports receipt of an MNPS forced takeover request.	Issue SETLOGON OPTCD=PERSIST, PARMS= (FORCETKO=MULTI) if just MNPS takeovers are to be supported, or PARMS= (FORCETKO=ALL) if both MNPS and SNPS takeovers are to be supported.
Initiate MNPS forced takeover processing by issuing OPEN ACB.	Specify (PARMS= (PERSIST=YES, FORCETKO=YES) on the ACB macroinstruction for the application. Issue OPEN ACB for application while the application is open on another host.
Ensure application supports MNPS forced takeover after recovery.	If the application is recovered on this node, the MNPS forced takeover capability support is inherited from the previous owning VTAM. So, even though the application is already ″persistence enabled″ after recovery, issue SETLOGON OPTCD=PERSIST, PARMS= (FORCETKO=MULTI) or PARMS= (FORCETKO=ALL) to set the MNPS forced takeover capability indicator to the desired level.
Optionally, indicate application support level for SNPS takeover requests.	Issue SETLOGON OPTCD=PERSIST, PARMS= (FORCETKO=SINGLE) if just SNPS takeovers are to be supported, or PARMS= (FORCETKO=ALL) if both MNPS and SNPS takeovers are to be supported. If SNPS takeovers are not supported, issue either SETLOGON OPTCD=PERSIST, PARMS= (FORCETKO=NONE) or PARMS= (FORCETKO=MULTI).

Stalled HPR pipe recovery

Problems in the data link control (DLC) layer used by an High-Performance Routing (HPR) PU may cause data flow to stall. A stalled HPR pipe solution is provided to detect the stall, inform the operator, and attempt to recover. Diagnostics are enhanced to provide information on the source of the problem.

When the HPR PU is using a High Performance Data Transfer (HPDT) DLC, recovery of the network layer packets (NLPs) causing the data flow stall is attempted. NLP recovery is always attempted for Enterprise Extender connections because Enterprise Extender is an HPDT DLC.

New messages are introduced to expose the problem:

- When a data flow stall is detected on an HPR PU
- When all NLPs causing the stall are acknowledged and therefore the data flow stall has been alleviated
- Every 30 seconds from the time the data flow stall is detected until the time it is alleviated
- In the replies to 'DISPLAY NET,ID=HPRPUName', 'DISPLAY NET,ID=HPRPUName,HPRDIAG=YES', and 'DISPLAY NET,RTPS'

Automatic HPR PU inactivation due to a persistent stall is not provided as in some cases data will again begin to flow without intervention. A decision to manually inactivate the HPR PU should be based on the messages provided.

Note: In many cases, a stalled HPR pipe is not an abnormal condition. For example, stalls may be reported while the HPR pipe is in the process of

pathswitching; or, in the case of Enterprise Extender, CPU intensive processing (such as TCP/IP dumping) may result in a stall being reported. These, and other factors, should be given consideration prior to contacting IBM service to report a stalled HPR pipe.

Restrictions

NLP recovery is not attempted for a stalled HPR PU when the connection is non-HPDT as the risk of attempting recovery in this environment is much greater.

What this change affects

- Availability
- Operations
- Diagnosis
- Storage

Using this function

You can perform the desired tasks in the following table.

Table 142. Stalled HPR pipe recovery

Task	Procedure	Reference
Determine if an HPR PU is currently, or ever has been, affected by a data flow stall.	Issue DISPLAY NET,ID=*HPRPUName*.	DISPLAY ID command in *z/OS Communications Server: SNA Operation*
Determine if backpressure has even been applied due to a stalled HPR PU.	Issue DISPLAY NET,ID=*HPRPUName*,HPRDIAG=YES.	DISPLAY ID command in *z/OS Communications Server: SNA Operation*
Determine all the currently stalled HPR PUs.	Issue DISPLAY NET,RTPS,STALL=YES.	DISPLAY RTPS command in *z/OS Communications Server: SNA Operation*
Determine if HPR PU inactivation is warranted.	Observe the IST1955I messages and, using the enhancements to the DISPLAY commands shown above, monitor the data flow state for the PUs reported in the message. If the data flow state is persistently stalled, or if IST1955I is observed to be consistent, recycling the HPR PU may be warranted.	*z/OS Communications Server: SNA Operation*

SNA/IP DISPLAY CSM enhancements

The CSM monitor function to monitor CSM buffers between the components of z/OS Communication Server was made available in V1R5; see "CSM buffer tracking" on page 223. In z/OS V1R6 Communications Server, a new DISPLAY CSMUSE command is available to evaluate the use of CSM.

Although the DISPLAY CSMUSE command is similar to the existing DISPLAY CSM, it provides a lower level of detail regarding storage usage; therefore, the information provided is different. The DISPLAY CSMUSE command provides displays of CSM that is being used by Communications Server components. Display of this information is intended to improve the serviceability of the z/OS Communications Server and to aid in CSM storage diagnosis.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Storage
- Usability

Using this function

The SNA/IP DISPLAY CSM enhancements does not require any action unless you want to take advantage of the function. If so, perform the desired tasks in the following table.

Refer to the DISPLAY CSMUSE command in *z/OS Communications Server: SNA Operation* for more information.

Table 143. SNA/IP DISPLAY CSM enhancements

Task	Procedure
Display the summary of CSM storage usage of pools by monitor ID.	Issue the DISPLAY NET,CSMUSE command.
Display the summary of CSM storage usage of owner ID by monitor ID.	Issue the DISPLAY NET,CSMUSE,OWNERID=xxxx command.
Display the detail of CSM storage usage of pool by monitor ID.	Issue the DISPLAY NET,CSMUSE,POOL=4KECSA command.

Chapter 8. V1R5 SNA new function summary

This chapter includes a section for every function or enhancement introduced for SNA in z/OS V1R5 Communications Server. The sections include the following 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. The tables include references to the documents that contain more detailed information for each task.

See Table 125 on page 177 for a complete list of the SNA functional enhancements of the current and recent releases.

Refer to *z/OS Migration* for information about how to maintain the functional behavior of previous releases. Refer to *z/OS Summary of Message and Interface Changes* for information on new and changed messages and interfaces.

General considerations

In the APPN Class of Service definitions, the range allowed to be coded on the WEIGHT parameter of the LINEROW definition statement used to be 0-255. This range has been changed to be 2-255.

APPN trace enhancement

z/OS V1R5 Communications Server introduces an enhancement to APPN tracing to aid in accurately diagnosing problems with an APPN LU-LU session. The enhancement consists of a new subtrace option (TGVC) that traces the TG Vectors sent for Request Route, Recompute Route, Request TG Vectors, and Cache Data messages.

Recommendation: Because of the potentially large amounts of data contained in the TG Vectors, IBM recommends that the new subtrace option (TGVC) be turned on only for problem diagnosis. Furthermore, it should only be turned on for the time required to generate the necessary documentation, then turned off.

Restrictions

None.

What this change affects

- Diagnosis
- Performance

Using this function

The APPN trace enhancement does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 144. APPN trace enhancement - Migration task

Task	Procedure	Reference
Activate/Terminate TGVC subtrace.	Issue MODIFY VTAM,TRACE/NOTRACE command with TYPE=VTAM,SUBTRACE=TGVC and OPT=SSCP or ALL.	*z/OS Communications Server: SNA Operation*

CSDUMP command enhancements

Prior to z/OS V1R5 Communications Server, the MODIFY CSDUMP command set triggers to take dumps but it did not issue a message to indicate the reason of the dump. Furthermore, there was no way to display current triggers or to allow the removal of a trigger when it was no longer needed.

z/OS V1R5 Communications Server enhances the CSDUMP command in the following ways:

- The CSDUMP processing will issue a new message that indicates the reason why a CSDUMP was triggered.
- The MODIFY CSDUMP command is also enhanced to allow the option to remove any or all of the existing CSDUMP triggers.
- A new DISPLAY CSDUMP command is available to display the current CSDUMP triggers.

Restrictions

None.

What this change affects

- Usability
- Diagnosis

Using this function

The CSDUMP command enhancements does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 145. CSDUMP command enhancements

Task	Procedure	Reference
Display the current CSDUMP triggers.	Issue the DISPLAY NET,CSDUMP command.	*z/OS Communications Server: SNA Operation*
Delete the active CSDUMP message or sense triggers.	Issue MODIFY CSDUMP,DELETE=ALL to delete the message and sense triggers. Issue MODIFY CSDUMP,DELETE=MESSAGE to delete only the message trigger. Issue MODIFY CSDUMP,DELETE=SENSE to delete only the sense trigger.	*z/OS Communications Server: SNA Operation*

DLUR message enhancements

z/OS V1R5 Communications Server introduces new messages for DLUR connectivity:

- DLUS accounting messages

  New messages are issued when a DLUR served physical unit begins or ends communication with its DLUS. In addition, if an INOP occurs that results in the inactivation of the SSCP to PU session, a new message is issued to identify the DLUR of the PU.

- DLUS serviceability aid

  When a negative response is received for a request, such as an ACTLU, DACTLU, ACTPU, or DACTPU, a message group is issued to indicate the failure. This message group begins with IST1139I. z/OS V1R5 Communications Server adds a new message to this message group to identify the name of the DLUR when the resource identified in IST1139I is served by a DLUR.

Refer to *z/OS Communications Server: SNA Messages* for information about messages.

Restrictions

DLUS serviceability aid messages require a MSGLEVEL=V4R1 or later.

What this change affects

- Connectivity
- Diagnosis
- Operations

Using this function

There are no migration procedures associated with this enhancement.

Enterprise Extender enhancements

z/OS V1R5 Communications Server enhances Enterprise Extender (EE) in the following areas:

- **Connection network diagnostics enhancement**

  A new message has been introduced to inform the operator when a dial fails or a connection INOPs over a virtual routing node (VRN).

  Prior to this enhancement, retries for a dial failure or an INOP for an existing connection that was routed over a connection network link would repeatedly fail without the operator knowing what virtual routing node was being used.

- **EE dial usability enhancement for Dynamic PUs**

  A new type of model PU can be defined for use as the model for dynamic non-connection-network PUs used for Enterprise Extender on the host receiving the dial. This allows the user flexibility in coding certain operands for this type of dynamic PU, which previously used default characteristics.

  Prior to this enhancement, having the same set of default characteristics used for each dynamically-created non-connection-network Enterprise Extender PU did not allow the user the flexibility to tailor values such as TG characteristics, the disconnect timer delay, or whether to attempt redial when connections for these dynamic PUs failed.

- **Multiple VRNs for Enterprise Extender**

z/OS V1R2 Communications Server provided an enhancement to allow Enterprise Extender connection networks to span multiple APPN subnetworks and/or NETIDs. In z/OS V1R2 Communications Server, you were limited to one local and one global connection network for Enterprise Extender connectivity. z/OS V1R5 Communications Server lifts this restriction. In addition, IPADDR (representing the local static VIPA address to be used for this Enterprise Extender connection) or HOSTNAME (representing the name to be resolved into the local static VIPA address) may now be coded on the Enterprise Extender GROUP definition statement. This allows Enterprise Extender connections to communicate from this host through multiple static VIPAs.

This enhancement benefits you because a single global virtual routing node is not sufficient in every case:

- Some configurations may involve two or more disjoint IP networks to which a given VTAM must connect. All nodes connected to a given VRN must, by definition, be able to connect directly to any other node also connected to that VRN. This restriction means that only one of the two IP networks can use a Connection Network, with the other network requiring manual definition of the connections from VTAM to every other node in that network.
- Different VRNs may need to support different link characteristics. For instance, a subset of users may require secure links, while others can use unsecure links.
- Depending on the requirements of the session, users need to connect to the S/390 using the different session characteristics. For example, some sessions may require secure connections, while others may require faster link speeds.

- **IPv6 and firewall support**

  z/OS V1R5 Communications Server provides the following capabilities:

  - Support is added to enable the use of IPv6 addressing for Enterprise Extender connections.
  - The capability to specify a hostname, instead of an IP address for Enterprise Extender definitions, is now provided. The remote endpoint receives the partner's hostname and performs name-to-address resolution on the hostname to obtain the correct IP address for Enterprise Extender connection establishment in a network where firewalls and network address translation is used. The ability to exchange hostnames, instead of IP addresses, allows Enterprise Extender connection networks to work with network address translation (NAT) firewalls.

    A new option, HOSTNAME, can be specified on definitions for the **local** host by the following:

    - Start option
    - GROUP in XCA major node

    HOSTNAME can continue to be specified on definitions for the remote host on the PATH statement in the switched major node. The value specified for HOSTNAME on the PATH statement must now be no longer than 64 characters, however.

    The use of HOSTNAME is not limited to Global Virtual Routing Nodes (GVRNs), but can also be used for local VRN connections and even predefined connections. The hostname processing is available with both IPv4 and IPv6 protocols.

- **New buffer pools**

  Two new buffer pools, T1BUF and T2BUF, have been added. Within the HPR-RTP component and when applicable, a T1BUF or T2BUF will be acquired

in lieu of a TIBUF. Therefore, the usage of the T1BUF and T2BUF pools will be inversely proportional to the usage of the TIBUF pool.

T1BUF

The T1BUF provides the area used by RTP to pre-append the HPR network and transport headers. By defining this area within the T1BUF, processing overhead incurred to acquire and release the storage for this area is eliminated. This efficiency is gained even when HPR is not using an Enterprise Extender connection.

When HPR is using an Enterprise Extender connection, the T1BUF also provides the area used by TCP/IP to pre-append the UDP and IP headers. By defining this area within the T1BUF, processing overhead incurred to acquire and release the storage for this area is eliminated.

When HPR is using an Enterprise Extender connection over a QDIO or iQDIO device driver, the T1BUF serves as a small packing buffer. Packing the headers and data exploits the media architecture.

T2BUF

The T2BUF provides all the benefits of the T1BUF, and in addition, contains a larger packing area. RTP will acquire a T2BUF in lieu of a T1BUF only when the Enterprise Extender connection is over a QDIO or iQDIO device driver and the estimated total size of the Enterprise Extender packet exceeds the size of the T1BUF packing area. In addition, RTP will always acquire a T2BUF in lieu of a T1BUF when retransmitting in this configuration.

The default values assigned to these two pools are intentionally conservative; therefore, monitoring the usage of these pools is recommended.

You can use T1BUF regardless of whether you are using Enterprise Extender. T2BUF, however, exclusively supports Enterprise Extender over an QDIO/iQDIO device driver.

You can monitor your buffer pool storage by using the DISPLAY BFRUSE command. You may modify the buffer pools to use your own definitions or you may choose to use the defaults.

Refer to *z/OS Communications Server: SNA Resource Definition Reference* for more information about buffer pools.

Restrictions

For multiple VRNs for Enterprise Extender, the restrictions of z/OS V1R2 Communications Server are still applicable. Those restrictions are repeated here for your convenience:

- Global Virtual Routing Nodes (GVRNs) will not allow dynamic connections to end nodes (ENs) that are being served by a branch extender (BrNN).
- A GVRN can be utilized when it is defined on the endpoint node, an EBN for the endpoint's network (or subnetwork), or under certain circumstances an NN in the network (or subnetwork) of the PLU. A GVRN defined on an NN can be utilized when it is in the PLU's network (or subnetwork) and the final session route determination is being performed in this network (NN located in the network of the OLU in a PLU-init scenario or the network of the DLU in an SLU-init scenario).
- A GVRN will not be used in intermediate networks (or subnetworks) along the session path. A GVRN can only be used in the network (or subnetwork) for the session endpoints.

- A GVRN will not be used in the session route when one of the endpoints resides in the subarea.

For IPv6 and firewall support for EE, the following restrictions apply:

- A given GVRN or local VRN connection must be defined to use either IPv4 or IPv6 protocols, but not both. If a node wants to support Enterprise Extender connections using both protocols, at least two VRNs (one IPv4 and one IPv6) must be defined.
- Enterprise Extender endpoints that will communicate must be enabled for the same Internet protocol, either IPv4 or IPv6.
- A particular hostname should resolve to a single static VIPA address when resolved by the host that owns the VIPA address. When the same hostname is resolved by a remote Enterprise Extender endpoint, the value should resolve to either the static VIPA address or to a network address translation (NAT) address suitable for reaching the ultimate Enterprise Extender endpoint that owns the hostname.
- When IPv6 protocols are to be used for an Enterprise Extender connection (either predefined or across a virtual node), you cannot code the IPv6 address explicitly on the appropriate SNA definition statements, but you must instead supply a hostname to be used for name-to-address resolution.

Dependencies

For Enterprise Extender connection networks, the following dependency applies:

- To exploit Global Connection Networks, a pure APPN session path is required with each border node on the path supporting extended subnetwork boundaries (EBNs). Each of these EBNs must be at z/OS V1R2 Communications Server or later level to support GLOBAL virtual routing nodes.

For IPv6 and firewall support for EE, the following dependency applies:

- The use of HOSTNAME requires name-to-address resolution capabilities using Domain Name Server (DNS) or local host tables.

What this change affects

- Availability
- Customization
- Diagnosis
- Installation
- Operations
- Usability

Using this function

Even if you do not intend to use the Enterprise Extender enhancements of z/OS V1R5 Communications Server, you should be aware of the following migration considerations:

- The IPADDR and TCPNAME start options are no longer valid if specified at a pure subarea node.
- The HOSTNAME operand on the PATH statement, if longer than 64 characters, will be rejected.

To take advantage of the Enterprise Extender enhancements, perform the desired tasks in the following table.

Table 146. Enterprise Extender enhancements

Task	Procedure	Reference
Define static VIPA addresses.	Add DEVICE/LINK/HOME statements (for IPv4) or INTERFACE statements (for IPv6) to the TCP/IP profile dataset to define the static VIPA addresses to the stack.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Define and start IUTSAMEH.	Do **one** of the following (they are mutually exclusive): • If you are *not* using DYNAMICXCF for IPv4, add DEVICE/LINK (and optionally HOME) and START statements (for IPv4) or INTERFACE and START statements (for IPv6) to the TCP/IP profile dataset to define and start IUTSAMEH. • If you are using DYNAMICXCF for IPv4, then code IPCONFIG6 DYNAMICXCF (for IPv6) to the TCP/IP profile dataset instead of defining an IPV6 IUTSAMEH interface. **Note:** A mix of static and dynamic IPv4 and IPv6 definitions for a device are not allowed. If a static IUTSAMEH IPv4 DEVICE/LINK is defined, then the IPv6 dynamic definition for IUTSAMEH will not be created; if a static IUTSAMEH IPv6 INTERFACE is defined, then the IPv4 dynamic definition for IUTSAMEH will not be created.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
Assign hostnames for accessing these addresses. Create both the name-to-address and address-to-name name server mappings.	Do the following: • Create DNS AAAA records mapping hostname to the IPv6 static VIPA address, or DNS A records for mapping hostname to an IPv4 static VIPA address, or add an entry mapping hostname to the appropriate address in the local host tables of all Enterprise Extender endpoints. • Create DNS PTR records to map the IPv6 address back to its corresponding hostname, or to map the IPv4 address back to its corresponding hostname, or add an entry mapping the static VIPA address to the correct hostname in the appropriate local address tables of all Enterprise Extender endpoints.	*z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*
If you wish to use IPv6 protocols for Enterprise Extender using the connection network model, define XCA major nodes that represent the IPv6 connections to your connection networks.	Code XCA major node definitions (PORT, GROUP and LINE statements) by doing the following: • Specify a VNTYPE of GLOBAL or LOCAL on the Enterprise Extender GROUP definition statement. • Specify the name of the VRN using the VNNAME operand on the GROUP, or optionally the PORT, statement. The same value for VNNAME must be coded on all Enterprise Extender nodes that wish to connect over this VRN. • Specify the type of the VRN using the VNTYPE operand on the GROUP, or optionally the PORT, statement. • Specify the **local** hostname associated with this VRN by coding HOSTNAME on the GROUP statement, or allow to default from the HOSTNAME start option. • Specify, if desired, a time value during which hostname resolution must be completed in order for activation to be successful, using the IPRESOLV operand on the GROUP statement.	*z/OS Communications Server: SNA Resource Definition Reference*

Table 146. Enterprise Extender enhancements (continued)

Task	Procedure	Reference
If you wish to use IPv4 protocols for Enterprise Extender using the connection network model, define XCA major nodes that represent the IPv4 connections to your connection networks.	Do the following: • Specify a VNTYPE of GLOBAL or LOCAL on the Enterprise Extender GROUP definition statement. • Specify a VNNAME (name that will be specified on all nodes defining the VRN). • Specify the IPADDR or HOSTNAME operand on the Enterprise Extender GROUP definition statement. The IPADDR specified here is the local IPv4 static VIPA address you want other Enterprise Extender nodes to use in order to communicate with this host by using this connection. Likewise, the HOSTNAME specified here is the name that would be resolved to the IPv4 static VIPA address you want other Enterprise Extender nodes to use in order to communicate with this host by using this connection. Alternatively, you can allow IPADDR and HOSTNAME to default from the start option setting. • Specify, if desired, a time value during which hostname resolution must be completed in order for activation to be successful, using the IPRESOLV operand.	*z/OS Communications Server: SNA Resource Definition Reference*
If you wish to use IPv6 protocols for Enterprise Extender using the predefined connection model, define switched major node representations of the connections to remote Enterprise Extender nodes.	Code switched major node definitions (PU, PATH): • Specify the **remote** hostname associated with this predefined connection by coding HOSTNAME on the PATH statement. The hostname cannot be longer than 64 characters. • Specify, if desired, a time value during which hostname resolution must be completed in order for activation to be successful, using the IPRESOLV operand. Prior to z/OS V1R5, the default setting was 45 seconds, but it is now 0 seconds (or no timeout value). Code XCA major node definitions (PORT, GROUP and LINE statements): • Specify the **local** hostname associated with this Enterprise Extender connection by coding HOSTNAME on the GROUP statement, or allow to default from the HOSTNAME start option.	*z/OS Communications Server: SNA Resource Definition Reference*

Table 146. Enterprise Extender enhancements (continued)

Task	Procedure	Reference
If you wish to use IPv4 protocols for Enterprise Extender using the predefined connection model, define switched major node representations of the connections to remote Enterprise Extender nodes.	Code switched major node definitions (PU, PATH): • Specify the **remote** static VIPA address associated with this predefined connection by coding IPADDR on the PATH statement, or specify the remote hostname to be used to acquire the remote static VIPA address associated with this predefined connection by coding HOSTNAME on the PATH statement. If HOSTNAME is used, the value specified can be no longer than 64 characters. • Specify, if desired, a time value during which hostname resolution must be completed in order for activation to be successful, using the IPRESOLV operand. Prior to z/OS V1R5, the default setting was 45 seconds, but it is now 0 seconds (or no timeout value). Code XCA major node definitions (PORT, GROUP and LINE statements): • Specify the **local** static VIPA address associated with this predefined connection by coding IPADDR on the GROUP statement, or specify the hostname to be used to acquire the local static VIPA address associated with this predefined connection by coding HOSTNAME on the GROUP statement. Alternatively, you can allow the value to default from the IPADDR or HOSTNAME start options.	*z/OS Communications Server: SNA Resource Definition Reference*
Customize Dynamic non-connection Network PUs used for Enterprise Extender.	Code a PU with the new DYNTYPE=EE specification in a model major node, setting allowable operands such as DISCNT, DWINOP and TG characteristics as desired.	*z/OS Communications Server: SNA Resource Definition Reference*
Use the new buffer pools, T1BUF and T2BUF.	You can use T1BUF regardless of whether you use Enterprise Extender. T2BUF is exclusive for Enterprise Extender over a QDIO/iQDIO device driver. You can monitor your buffer pool storage and modify it if desired. The new buffer pools are included in the DISPLAY BFRUSE command output.	*z/OS Communications Server: SNA Resource Definition Reference*
Activate the VTAM and TCP stacks.	Issue the START commands for VTAM and TCPIP.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: IP System Administrator's Commands*
Activate the Enterprise Extender Virtual Routing Node.	Do the following steps: 1. Activate the XCA Major Node for Enterprise Extender (if not already active) 2. Activate at least one line (in the Enterprise Extender XCA Major Node) from the GROUP associated with that Virtual Routing Node.	*z/OS Communications Server: SNA Network Implementation Guide*

Table 146. Enterprise Extender enhancements (continued)

Task	Procedure	Reference
Activate the XCA or switched major nodes.	Issue VARY ACT commands, specifying the correct major node name: • Activate the GROUP definition and at least one LINE under that GROUP. • Activate the switched major node definition. • Establish the dial connection to the remote Enterprise Extender node.	*z/OS Communications Server: SNA Operation*
Verify that the correct IP addresses or HOSTNAME information is being utilized.	Issue DISPLAY ID=major_node_name and DISPLAY VTAMOPTS commands. If the VTAM start options are not correct, they may be modified by using MODIFY VTAMOPTS.	*z/OS Communications Server: SNA Operation*
Route around a failing connection network Virtual Routing Node (VRN) path from this node to a partner node until the connection network problem is corrected. Correcting the problem may involve taking similar actions and/or following established problem determination procedures at the partner node to correct the problem there.	If new message IST1903I is seen, do the following steps: 1. Note the VRN name and the partner node CP name in the message. 2. Activate an alternate non-connection-network path to reach the partner node given in the message, or ensure an alternate path is already available. 3. If PSRETRY is currently enabled for this node, issue MODIFY VTAMOPTS,PSRETRY=(0,0,0,0) to keep existing RTPs from path switching away from the VRN. Note that some or all of these RTPs may be using the VRN to reach different partners and may not be having any problems, so this step is taken so that the following steps will not unnecessarily impact RTPs that are functioning normally. 4. Do **one** of the following: a. Issue MODIFY TOPO,FUNCTION=QUIESCE for the VRN named in IST1903I. This is the recommended method. b. Issue VARY INACT for all lines to this VRN. c. Issue MODIFY TGP for the VRN to increase the weight of the path using the VRN above the weight of the alternate path. 5. Reissue the request that either generated the failing dial or originally created the INOPed connection. At this point, because of actions taken in step 4, an alternate path to the partner node will be chosen and the dial should succeed or the existing connection will be restored. Existing RTPs that were using the VRN and are still path switching will require no additional operator intervention after step 4 to switch to the new path. 6. Diagnose the problem with the connection network path between this node and the partner and correct it. This may involve taking action at the partner node. 7. Issue MODIFY TOPO,FUNCTION=NORMAL for the VRN, reactivate the VRN link, or decrease the path weight associated with the VRN as appropriate to reverse the action taken in step 4. 8. Enable or re-enable PSRETRY if desired. If the path weight of the re-enabled VRN is less than that of the alternate path referred to in step 2, then RTPs using the alternate path will now automatically switch to the VRN path.	*z/OS Communications Server: SNA Messages*, *z/OS Communications Server: SNA Operation*, and *z/OS Communications Server: SNA Resource Definition Reference*

RTP display enhancement

z/OS V1R5 Communications Server enhances the DISPLAY NET,RTPS command. This enables an operator to filter the HPR pipe displays and limit the output of the display.

New filters were added to allow for displaying RTPS by characteristics associated with the first hop:

- TG number
- CPNAME
- Adjacent Link Station name

Restrictions

None.

What this change affects

- Diagnostics
- Operations

Using this function

If you wish, you may limit the D RTPS output by specifying the FIRSTCP/FIRSTTG operands, or the ALSNAME operand, to retrieve a list of RTPs using the specified TG (or ALS) as the first hop.

Session setup and problem determination enhancements

z/OS V1R5 Communications Server provides three areas of enhancement for session setup and problem determination:

- **DSIRFMSG start option**

  Enhances the ability to receive the IST663I message group when the search to locate a session partner fails. DSIRFMSG controls whether the IST663I message group is displayed for searches that may not result in a session being established, such as searches that result when an application program issues INQUIRE OPTCD=APPSTAT.

  Tip: The DSIRFMSG function is driven when SIRFMSG= is coded on CDRSC definitions. Therefore, you may see an increase in the number of messages for resources that you currently have defined with SIRFMSG=.

  The DSIRFMSG start option will accept three values: NONE, OLUSSCP and ALLSSCP. The default is NONE because of the potentially large volume of messages.

- **Allow non-sysplex network nodes (NNs) for generic resource (GR) end nodes (ENs)**

  This enhancement allows the generic resource function on an end node to continue to operate while being served by a network node that is not in the same (or any) sysplex.

  Prior to this enhancement, the network node server for end nodes running generic resource applications had to be connected to the same coupling facility structure as the served end nodes. Two network node servers in each sysplex configuration were required to avoid a single point of failure. With this enhancement, you are allowed the flexibility of having a backup network node server that is not connected to the same sysplex as the served end nodes. The

applications on the served end nodes continue to support the generic resource function, including session level load balancing.

- **SSCPORD search option**

  This search option provides VTAM the ability to search ADJSSCP tables in a specified order. This allows for more granular control over network search order for resources. SSCPORD can be specified as a VTAM start option or in the ADJSSCP table as an operand on the NETWORK and CDRM statements.

Restrictions

The allow non-sysplex NNs for GR ENs enhancement has the following restriction:

- When end nodes supporting generic resources are using a backup network node server that is not connected to the same sysplex, all end nodes connected to the same generic resource structure must be served by the same backup network node server.

The DSIRFMSG start option and the design to allow SSCPORD on ADJSSCP tables do not have any restrictions.

Co-existence requirements

The DSIRFMSG start option and the design to allow SSCPORD on ADJSSCP tables do not have any co-existence requirements.

The allow non-sysplex NNs for GR ENs enhancement has the following co-existence requirement:

- All end nodes, supporting generic resources, that are connected to the same sysplex must have this function implemented. If all end nodes do not have this function installed the generic resources function will not work with a network node server that is not connected to the same generic resource structure.

What this change affects

- Availability
- Operations
- Diagnosis
- Usability
- Performance

Using this function

If you want to use the DSIRFMSG start option enhancement, perform the tasks in the following table.

Table 147. DSIRFMSG start option enhancement

Task	Procedure	Reference
For diagnosis, enable the display of search failure messages for searches that may not result in sessions being established.	Specify DSIRFMSG=ALLSSCP or OLUSSCP on the START command or using the MODIFY VTAMOPTS command.	*z/OS Communications Server: SNA Resource Definition Reference*
After diagnosis of search failures, disable the display of search failure messages for searches that may not result in a session being established.	Specify DSIRFMSG=NONE on the START command or using the MODIFY VTAMOPTS command.	*z/OS Communications Server: SNA Resource Definition Reference*

If you want to allow non-sysplex NNS for GR ENs, perform the tasks in the following table.

Table 148. Allow non-sysplex NNS for GR ENs enhancement

Task	Procedure	Reference
Define backup network node server outside the sysplex for generic resource support.	Code ENBCAST=YES operand on the entry for the backup network node server in the network node server list.	*z/OS Communications Server: SNA Resource Definition Reference*

If you want to use SSCPORD on ADJSSCP tables, perform the task in the following table.

Table 149. Allow SSCPORD on ADJSSCP tables - Migration task

Task	Procedure	Reference
Control the order in which session requests are routed when using ADJSSCP tables.	Code SSCPORD= as a VTAM start option or on NETWORK and/or CDRM statements in the ADJSSCP table.	*z/OS Communications Server: SNA Resource Definition Reference*

Sift-down support for model major nodes

z/OS V1R5 Communications Server adds the ability to sift parameters for model LU definition statements in the model major node. LU keywords may be coded on a new GROUP definition statement so they can sift down to subsequent LU definition statements. This can help to reduce repetitive definitions for model LUs.

Restrictions

There is no support for sifting to or from PU definition statements.

Coding LU keywords on PU definition statements in the model major node is not allowed. Coding PU keywords on the GROUP definition statement is not allowed.

What this change affects

- Usability

Using this function

If you want to use the sift-down support for model major nodes, perform the task in the following table.

Table 150. Sift-down support for model major nodes - Migration task

Task	Procedure	Reference
Sift LU keyword values from a GROUP definition statement in a model major node.	Code a GROUP definition statement that contains the LU keywords that are to be sifted down to LUs in the GROUP.	*z/OS Communications Server: SNA Resource Definition Reference*

Storage management enhancements

z/OS V1R5 Communications Server introduces a new VTAM modify command to allow the IO Buffer pool expansion limit parameter to be modified without the need to recycle VTAM. Prior to this enhancement, when the IO Buffer pool expanded to its defined limit, VTAM stopped sending and receiving data and frequently had to be recycled to recover and to increase the IO buffer pool specifications.

Restrictions

The *xpanno*=0 must not have been specified in an IOBUF start list or the VTAM start command. Expansion limit is invalid when IO buffer pool static buffering is in effect.

What this change affects

- Availability
- Storage

Using this function

If you want to use the storage management enhancements, perform the task in the following table.

Table 151. Storage management enhancements - Migration task

Task	Procedure	Reference
Update the IO Buffer Pool expansion limit.	Issue MODIFY procname,BFRUSE,BUF=IOBUF, XPANLIM=value.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Resource Definition Reference*

Support for concurrent APING commands

z/OS V1R5 Communications Server includes enhanced support for APING commands, as follows:

- More than one DISPLAY APING command can be active concurrently. This means you can now issue a subsequent DISPLAY APING if the first one has not completed. This benefits testing by allowing the exchange of data over several sessions to various target LUs or to the same LU.
- Enhances the existing DISPLAY APINGDTP command to provide information on active sessions with the APINGD transaction program, allowing quicker operator termination of transactions which may be hung.
- Two new commands, DISPLAY APINGTP and MODIFY APINGTP, provide the same control and display capabilities for the APING command transaction program that already existed for the APINGD target transaction program. These new commands allow the setting and displaying of the instance limit for the APING command transaction program, and give the ability to optionally see the session identifier of each session that is being used for APING transactions. The maximum number of sessions that VTAM displays for the DISPLAY,NET APINGTP command can be limited by the MAX operand.
- Allows suppression of iteration statistics messages.

Restrictions

Executing large numbers of DISPLAY APING commands at the same time may have performance impacts on other system processing.

What this change affects

- Operations
- Usability

Using this function

If you want to use the support for concurrent APING commands, perform the tasks in the following table.

Table 152. Support for concurrent APING commands

Task	Procedure	Reference
Change the number of DISPLAY APING commands which are allowed to execute concurrently.	Issue MODIFY APINGTP,INSTANCE=limit where limit is the desired maximum number of concurrent DISPLAY APING commands.	*z/OS Communications Server: SNA Operation*
Display information about the APING **command** transaction program.	Issue DISPLAY APINGTP command. LIST=ALL will show the instance limit, the number of active sessions, and the LU name and Session ID of each session. LIST=COUNT will show the instance limit and the number of active sessions. LIST=ONLY (or no LIST value) will show only the instance limit.	*z/OS Communications Server: SNA Operation*
Display information about the APINGD **target** transaction program.	Issue DISPLAY APINGDTP command. LIST=ALL will show the instance limit, the number of active sessions, and the LU name and Session ID of each session. LIST=COUNT will show the instance limit and the number of active sessions. LIST=ONLY (or no LIST value) will show only the instance limit.	*z/OS Communications Server: SNA Operation*
Initiate an APING transaction to another LU in the network.	Issue DISPLAY APING,ID=luname where luname is the name of the target LU. LIST=ALL will show route information for the transaction session, statistics for setting up the transaction, detailed statistics for each send and receive iteration, and averages and totals for the complete transaction. LIST=SUMMARY will show route and setup information, as well as averages and totals for the complete transaction, but will omit the detailed iteration statistics messages.	*z/OS Communications Server: SNA Operation*

SWNORDER enhancements

The SWNORDER and DLRORDER parameters that can be specified as start options or on the XCA and NCP major nodes have been enhanced to allow greater control over PU selection during connection processing. To accomplish this, a second operand has been added to the existing format. This new operand can restrict the selection of a PU for the connection to the value specified by the first operand. By specifying SWNORDER and DLRORDER on the XCA or NCP major nodes, the start option value can be overridden on a line-by-line basis.

Prior to this enhancement, when a node dialed in and the PU was not found using STATNID, VTAM could find a PU using the CPNAME even though SWNORDER was defined to use STATNID first. The connection was established, even though the IDBLK/IDNUM did not match the found PU's definition. Later, when the resource that the PU definition represented attempted a connection, the connection failed because the PU is already in use. This enhancement will eliminate this availability problem.

The MODIFY VTAMOPTS command may be used to change either or both parameters of the SWNORDER or DLRORDER start option while VTAM is active.

Restrictions

None.

What this change affects

- Operations
- Availability

Using this function

If you want to maintain the current SWNORDER function, no definition changes or migration actions are required. If you want to use the new START OPTION SWNORDER value, perform the desired tasks in the following table.

Table 153. Using the new START OPTION SWNORDER value

Task	Procedure	Reference
Globally limit the connections to use only the CPNAME of the input connection request.	Specify SWNORDER=(CPNAME,ONLY) in the VTAM START OPTIONS.	*z/OS Communications Server: SNA Resource Definition Reference*
Globally limit the connection to use only the IDBLK/IDNUM of the input connection request.	Specify SWNORDER=(STATNID,ONLY) in the VTAM START OPTIONS.	*z/OS Communications Server: SNA Resource Definition Reference*
Globally define the PU selection with SWNORDER, but restrict the selection for some LINEs in the XCA or NCP major nodes.	Perform the task of your choice: • Globally limit the PU selection to match the CPNAME by specifying SWNORDER=(CPNAME,ONLY) in the VTAM START OPTIONS. • Modify the selection for some lines to match CPNAME first but also permit STATNID by specifying SWNORDER=(,FIRST) on the GROUP or LINE definition to override the second parameter of the VTAM START OPTION.	*z/OS Communications Server: SNA Resource Definition Reference*

If you want to maintain the current DLRORDER function, no definition changes or migration actions are required. If you want to use the new START OPTION DLRORDER value, perform the desired tasks in the following table.

Table 154. Using the new START OPTION DLRORDER value

Task	Procedure	Reference
Globally limit the DLUR connections to use only the CPNAME of the input connection request.	Specify DLRORDER=(CPNAME,ONLY) in the VTAM START OPTIONS.	*z/OS Communications Server: SNA Resource Definition Reference*
Globally limit the DLUR connections to use only the IDBLK/IDNUM of the input connection request.	Specify DLRORDER=(STATNID,ONLY) in the VTAM START OPTIONS.	*z/OS Communications Server: SNA Resource Definition Reference*

Trace performance enhancements

z/OS V1R5 Communications Server introduces a new VTAM internal trace record, COPY, in the data space trace table. This new trace record contains statistical information about the amount of trace copied to the data space table, ISTITDS1, from the ECSA trace table. This will assist in determining the status and efficiency of the copying of trace records to the trace data space.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

There are no migration tasks or procedures associated with this enhancement; it is automatically enabled. The new trace entry, COPY, is generated as a default, and is not associated with any VTAM internal trace option.

Transmission subsystem enhancements

z/OS V1R5 Communications Server enhances SNA transmission subsystems in the following three areas:

- "HPR resequencing optimization"
- "MAXSLOW parameter for slowdown monitoring" on page 220
- "HPDT packing" on page 220

HPR resequencing optimization

The HPR resequencing optimization solution in z/OS V1R5 Communications Server significantly improves inbound processing of out-of-order and segmented HPR packets. HPR often uses unreliable or multi-link transmission group connections which tend to drop or cause out-of-order presentation of packets to the destination RTP endpoint.

HPR resequencing optimization also provides for enhanced serviceability of the HPR out-of-order sequence queue with the addition of two new VIT records (DAPT and OOSx). These records are added to the HPR VIT option.

Restrictions

None.

What this change affects

- Diagnosis
- Performance
- Storage

Using this function

There are no controls for HPR resequencing optimization as it is automatically enabled for inbound segmented or out-of-sequence HPR packets. However, to control the serviceability features of the enhancement, use the task provided in the following table. Refer to *z/OS Communications Server: SNA Operation* for more information.

Table 155. HPR resequencing optimization - Migration task

Task	Procedure

Activate the HPR VIT Option.
 	
The DAPT and OOSx VIT records are contained within the HPR VIT Option. In order to capture these events, the HPR VIT Option must be active.
	Issue the following to start recording of the DAPT and OOSx VIT records:
	`MODIFY procname,TRACE,TYPE=VTAM,MODE=mode,OPTION=HPR`
	
	Issue the following to stop recording of the DAPT and OOSx VIT records:
	`MODIFY procname,NOTRACE,TYPE=VTAM,MODE=mode,OPTION=HPR`

MAXSLOW parameter for slowdown monitoring

z/OS V1R5 Communications Server provides new slowdown monitoring and operator awareness for XCA subchannels by introducing a MAXSLOW parameter to allow a second time value. This second time value is the number of seconds an XCA subchannel is allowed to remain in a slowdown condition before the operator is notified of the slowdown condition. The default value for detecting an extended period of an XCA subchannel slowdown is 180 seconds.

Prior to this function, an operator could not determine and was not made aware that an XCA subchannel was in slowdown.

The MAXSLOW parameter is specified on the XCA port definition statement where a CUADDR is specified.

Restrictions

None.

What this change affects

- Operations

Using this function

If you want to use the new MAXSLOW parameter for slowdown monitoring, perform the tasks in the following table.

Table 156. MAXSLOW parameter for slowdown monitoring

Task	Procedure	Reference
Determine if an XCA device is in slowdown.	Issue the following command: `DISPLAY NET,ID=xca_major_node` The message IST1885I indicates SLOWDOWN=YES|NO.	*z/OS Communications Server: SNA Operation*
Set the slowdown time value for an XCA device to 200 seconds for operator notification.	Code MAXSLOW=(,200) on the XCA major node.	*z/OS Communications Server: SNA Resource Definition Reference*

HPDT packing

For point-to-point connections using the High Performance Data Transfer (HPDT) Multi-Path Channel (MPC) protocol, throughput of small SNA or Enterprise Extender data packets can be significantly improved by enabling HPDT packing. This solution provides for better utilization of the HPDT MPC data stream by eliminating all of the alignment bytes transmitted in the HPDT data segment.

A new PACKING operand is provided on the TRLE definition statement to allow for control of HPDT packing.

Recommendations

IBM strongly recommends that you read the HPDT packing section in *z/OS Communications Server: SNA Network Implementation Guide* to take advantage of this function and to become aware of its dependencies.

Restrictions

HPDT packing is only implemented for non-XCF point-to-point connections; therefore XCF, ATM, and OSA devices are excluded.

What this change affects

- Performance
- Storage

Using this function

If you want to enable, disable, or tune HPDT packing, perform the desired tasks in the following table.

Table 157. Enabling, disabling, and tuning HPDT packing

Task	Procedure	Reference
Enable HPDT packing for a point-to-point MPC connection.	Add PACKING=ON or PACKING=max_pdu_size to the MPC TRLE definition deck.	*z/OS Communications Server: SNA Resource Definition Reference*
Disable HPDT packing for a point-to-point MPC connection.	Remove the PACKING= operand from the MPC TRLE definition deck or code PACKING=OFF.	*z/OS Communications Server: SNA Resource Definition Reference*
Tune HPDT packing.	Vary the max_pdu_size value and use VTAM Tuning Statistics or similar sniffer to measure throughput. Simultaneously measure CPU and channel utilization. When measuring using TNSTATs with a consistent, repeatable data stream, the OPDU to write device BYTECNT ratio should be maximized with no significant adverse effects on throughput or CPU utilization.	*z/OS Communications Server: SNA Resource Definition Reference* and *z/OS Communications Server: SNA Network Implementation Guide*

IPv6 support for SNA display of IP addresses

VTAM supports the association of LU names with IP addresses when the APPL, LU, or CDRSC represents a TN3270 client. In z/OS V1R5 Communications Server, the TN3270 server supports IPv6 addresses. In addition, VTAM functions that provide the LU name and IP address association now support IPv6 addresses.

Restrictions

None.

Incompatibilities

The following incompatibilities must be considered:

- Changed messages. Applications that process the following messages must plan for the described changes:

  - IST1669I IPADDR..PORT ipaddr..portno - This message is part of a group of messages issued in response to a DISPLAY ID command for a TN3270 client LU , application resource, or CDRSC, or for a DISPLAY ID,IDTYPE=IPADDR command when only one TN3270 client LU or application is associated with the specified IP address. It is also part of the IST075I message group issued for DISPLAY NET,TSOUSER. The ipaddr may now be either an IPv4 address displayed in dotted decimal or an IPv6 address displayed as colon hexadecimal.
  - IKT122I IPADDR..PORT ipaddr..portno - TSO/VTAM issues this message when a TN3270 client attempts to log on to TSO/VTAM but fails to do so. The ipaddr may now be either an IPv4 address displayed in dotted decimal or an IPv6 address displayed as colon hexadecimal.
- When the SNA portion of the TN3270 session is cross-domain and the host where the PLU resides is downlevel (at least to Communications Server for OS/390 V2R10), the host where the PLU resides is not able to display an IPv6 address. Therefore, it would not display IP information for DISPLAY ID commands for CDRSC or for a DISPLAY ID, IDTYPE=IPADDR. Also, any VTAM exits that are associated with this session, such as LOGON or Session Management Exit, would not receive the TCP/IP Information Control Vector as input.
- Users of the TSO GETTERM macro that request IPADDR or DOMAIN information but have not made changes to support IPv6 information could receive unpredictable results as output from this macro if the TN3270 client represents an IPv6 address. In this case, the IP address returned will be X'FFFFFFFF'. The port and the DNS name information (if present) will be returned.

  Refer to *z/OS TSO/E Programming Services* for information on changes needed to support IPv6.
- TSO/VTAM exit IKTCASX1 — The IKTCASX1 exit parameter list structure, IKTWESTD contains the IP address of an associated TN3270 client in the WE_IP_ADDR field. Until now, this address could only be an IPv4 address. VTAM now supports an LU that is associated with an IPv6 TN3270 client. If the client is IPv6 and the exit has not been modified to support IPv6, the WE_IP_ADDR field will contain X 'FFFFFFFF', making the real IP address unavailable. To resolve this incompatibility, refer to *z/OS Communications Server: SNA Customization* for changes needed to support IPv6.
- USSMSG macro Buffer operand — Prior to z/OS V1R5 Communications Server, the USSMSG macro's BUFFER operand allowed for IP address substitution using @@@@@@@@@IPADDR, which represents the length of a textual IPv4 address. If an existing USSMSG BUFFER is coded to specify this string, but the IP address associated with the TN3270 client is an IPv6 address, the address will be replaced with the text IPV6 ADDRESS, making the real client IP address unavailable. Refer to *z/OS Communications Server: SNA Resource Definition Reference* for the new IPv6 substitution string.

What this change affects

- Application development
- Customization
- Operations
- Usability

Using this function

If you want to use the IPv6 support for SNA display of IP addresses, perform the tasks in the following table.

Table 158. IPv6 support for SNA display of IP addresses

Task	Procedure	Reference
Allow the VTAM Session Management Exit (SME) functions of session authorization and session accounting to report on a session with an LU that represents an IPv6 TN3270 client.	Modify the SME to handle the new IPv6 address in the IP Characteristics vector (CV'81'X). It is a subvector on the TCP/IP Information Control vector (CV'64'X) which is passed as an existing parameter to the SME for the authorization and accounting functions. Process the new IPv6 Zone Identification vector (CV'86'X) parameter that may be passed to the SME authorization and accounting functions when the IP Characteristics vector describes a session that is associated with an IPv6 TN3270 client.	*z/OS Communications Server: SNA Customization*
Allow the Logon Exit (also supported for TSO/VTAM) to support LUs that are associated with an IPv6 TN3270 client.	Modify the Logon Exit to handle the new IPv6 address provided in the IP Characteristics vector that is passed as a subvector on the TCP/IP Information Control vector (CV '64'X) as part of the CINIT RU. The logon exit can process a new IPv6 Zone Identifier vector (CV'86'X) that may be passed on the TCP/IP Information Control vector (CV '64'X) when the IP Characteristics vector contains an IPv6 address.	*z/OS Communications Server: SNA Customization*
Allow CMIP Topology Managers to support an LU that is associated with an IPv6 TN3270 client.	Modify CMIP Topology Managers to accept the LU attribute of tn3270ClientIpAddress. It has been expanded to allow a CMIP Topology Manager to display an LU that is associated with an IPv6 TN3270 client.	*z/OS Communications Server: CMIP Services and Topology Agent Guide*
Allow the TSO/VTAM exit IKTCASX1 (Error Handling for Non-Supported Terminals) to build logon failure messages for terminals associated with an IPv6 TN3270 client.	Modify IKTCASX1 to pass a new pointer to the TCP/IP Information Control Vector (CV X'64') in the IKTWESTD.	*z/OS Communications Server: SNA Customization*
Allow TSO to obtain IPv6 addresses associated with TN3270 session terminals.	Modify the GETTERM TSO macro invocation to return IPv6 information.	*z/OS TSO/E Programming Services*
Allow a USS Table to support IPv6 addresses associated with TN3270 session terminals.	Modify the USSMSG BUFFER operand to support client IP addresses that are IPv4 or IPv6.	*z/OS Communications Server: SNA Resource Definition Reference*

CSM buffer tracking

In z/OS V1R5 Communications Server, the CSM monitor function is available to monitor CSM buffers between many components of z/OS Communications Server. This function will be used by IBM Software Support to help diagnose CSM storage problems.

This function can be controlled using the Modify CSM command with the MONITOR operand. The valid options are MONITOR=ON, MONITOR=OFF and MONITOR=DYNAMIC. If the user chooses the option MONITOR=DYNAMIC, CSM buffer monitoring will be dynamically activated and inactivated. CSM will dynamically activate CSM buffer monitoring when CSM storage usage approaches the critical level. It will dynamically inactivate CSM buffer monitoring when CSM storage returns to a level slightly lower than the normal level. The critical level

storage usage is 90% or higher of ECSA MAX or FIXED MAX values specified in CSM parmlib IVTPRM00. The normal level storage usage is 85% or below of ECSA MAX or FIXED MAX values. It can be displayed to determine the status of the function using Display CSM with the MONITOR operand.

Restrictions

None.

What this change affects

- Diagnosis
- Operations
- Storage

Using this function

The CSM buffer tracking enhancement does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

The default value for CSM MONITOR is DYNAMIC. IBM recommends that you keep the CSM MONITOR value as DYNAMIC. If you choose to maintain the CSM behavior of previous releases, you can turn CSM MONITOR off using the following command: MODIFY procname,CSM,MONITOR=OFF.

Table 159. CSM buffer tracking

Task	Procedure	Reference
Activate/Inactivate CSM monitor function.	Issue MODIFY procname,CSM,MONITOR=YES to start the CSM MONITOR function. Issue MODIFY procname,CSM,MONITOR=NO to stop the CSM MONITOR function. Issue MODIFY procname,CSM,MONITOR=DYNAMIC to monitor CSM storage dynamically.	*z/OS Communications Server: SNA Operation*
Display the CSM MONITOR function.	Issue DISPLAY NET,CSM,MONITOR.	*z/OS Communications Server: SNA Operation*
Format the dump using CSMCMPID.	Under IPCS VTAMMAP Panel, use CSMCMPID(compid) to format CSM control blocks.	*z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*

Improve diagnostics for DLC dumps

During recovery, the dump process may dump additional information requiring fewer problem recreations to obtain problem documentation. For dumps generated from VTAM data link layer (DLC) processes, in some cases, both VTAM and TCP address spaces will be dumped. In z/OS V1R5 Communications Server, the VIT dataspace and TCP/IP CTRACE dataspace may also be included in the dump. This provides a more useful dump.

Restrictions

None.

What this change affects

- Diagnosis

Using this function

The improve diagnostics for DLC dumps enhancement does not require any action. Because more information is now dumped, you may need to examine the current size of your dump datasets and increase them if necessary.

OSA performance enhancements

z/OS V1R5 Communications Server introduces new TCP/IP configuration parameters that can override the values on the QDIOSTG and IQDIOSTG VTAM start options on a per-device basis. This allows you to better tune the system to optimize Communications Server fixed storage utilization.

Restrictions

None.

What this change affects

- Customization
- Storage

Using this function

The OSA performance enhancements do not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 160. OSA performance enhancements

Task	Procedure	Reference
Override the global QDIOSTG or IQDIOSTG value on a per-device basis to control the amount of storage used for read processing for an OSA-Express QDIO or HiperSockets interface.	Specify the READSTORAGE parameter on the LINK statement for IPAQENET, IPAQTR, or IPAQIDIO and/or the INTERFACE statement for IPAQENET6 in the TCP/IP profile.	*z/OS Communications Server: IP Configuration Reference*
Determine the amount of storage being used for read processing for an OSA-Express QDIO or HiperSockets TRLE.	Inspect the DISPLAY TRL output for an OSA-Express QDIO or HiperSockets TRLE.	*z/OS Communications Server: SNA Operation*

VTAM INOPDUMP enhancement

VTAM INOPDUMP was enhanced in z/OS V1R4 Communications Server; see "VTAM INOPDUMP enhancement" on page 244. In z/OS V1R5 Communications Server, it is further enhanced by introducing more granular control of whether an inoperative condition (InOp) will result in a dump being taken. This granularity is provided by the introduction of a new, separately controlled InOpCode function. InOpDump continues to control the scope of the resources that are enabled for dumping and InOpCode controls the conditions for which these resources will initiate a dump.

Each InOp reason code used by VTAM is now assigned a dump attribute that can be set to either DUMPENABLE or DUMPDISABLE. The InOpCode function is used to alter and display these dump attributes.

When an InOp occurs, a dump is taken only when both of the following conditions are true:

- The resource is enabled for InOpDump.
- The dump attribute for the specific InOp reason is DUMPENABLED.

Default dump attributes are provided automatically and internally. These defaults allow the InOpDump function to operate as in previous releases. A handful of InOp codes exists whose dump attribute defaults to DUMPDISABLE but the majority of InOp codes default to DUMPENABLE.

The InOpCode function is provided using a new modifiable VTAM start option and a new DISPLAY command.

Restrictions

With the exception of the ALL parameter, alteration of the attributes for multiple InOp codes cannot be done with a single start option or modify command.

Incompatibilities

InOpDump will not provide a dump unless the InOpCode identifying the condition is also enabled. However, the defaults provided ensure that InOp reason codes that were enabled for dumping in previous releases continue to be enabled and those disabled in previous releases continue to be disabled. Thus, if the InOpCode function is not used, InOpDump will perform as it has in previous releases.

Dependencies

The InOpDump and InOpCode functions are interdependent, meaning that a dump will be taken only when the resource is enabled for InOpDump and when the InOp code is dump enabled. If either is not enabled, dumping is bypassed.

What this change affects

- Customization
- Diagnosis
- Usability
- Availability
- Operations

Using this function

The following scenario is an example of how to acquire a dump for a specific inoperative condition. Unless the user is familiar with the interdependencies of the InOpDump and InOpCode functions, it is not recommended this type of procedure be performed without the assistance of VTAM service. Additionally, the procedures shown below are unique diagnostic procedures and should be performed only when documentation is required for an error that has previously occurred.

The following procedure shows how to determine all the VTAM InOpCodes and their attributes. If none of the attributes have been modified, this will also show the IBM default attribute values.

Table 161. VTAM INOPDUMP enhancement - Example of how to determine all the VTAM InOpCodes and their attributes

Task	Procedure	Reference
Display all VTAM InOpCodes and their attributes.	Issue DISPLAY NET,INOPCODE,MAX=* .	*z/OS Communications Server: SNA Operation*

The following procedures show how to override the ISTTSC8E InOp code 202 IBM default dump attribute of DumpEnable.

Table 162. VTAM INOPDUMP enhancement - Example of how to override the ISTTSC8E InOp code 202 IBM default dump attribute of DumpEnable.

Task	Procedure	Reference
At VTAM start time, disable ISTTSC8E InOp code 202 for dumping.	Add INOPCODE= (ISTTSC8E,202,DUMPDISABLE) to your start list or start command line.	*z/OS Communications Server: SNA Resource Definition Reference*
After VTAM initialization, disable ISTTSC8E InOp code 202 for dumping.	Issue MODIFY *procname*,INOPCODE= (ISTTSC8E,202,DUMPDISABLE).	*z/OS Communications Server: SNA Operation*

The following procedures show how to enable InOpDump only for a specific inoperative code on a specific TRLE. ISTLLCWC InOp reason code 100 and TRLE1 are used for the example.

Table 163. VTAM INOPDUMP enhancement - Example of how to enable InOpDump only for a specific inoperative code on a specific TRLE.

Task	Procedure	Reference
Disable InOpDump.	Issue MODIFY *procname*,INOPDUMP=OFF.	*z/OS Communications Server: SNA Operation*
Disable all InOpCodes from dumping.	Issue MODIFY *procname*,INOPCODE=(ALL,ALL,DUMPDISABLE).	*z/OS Communications Server: SNA Operation*
Enable the target InOpCode. (It is the only one that can possibly result in a dump.)	Issue MODIFY *procname*,INOPCODE= (ISTLLCWC,100,DUMPENABLE).	*z/OS Communications Server: SNA Operation*
Check all ISTLLCWC InOpCodes to ensure code 100 is the only one whose dump attribute is DumpEnable.	Issue DISPLAY NET,INOPCODE,MODULE=ISTLLCWC,MAX=*.	*z/OS Communications Server: SNA Operation*
Enable InOpDump for TRLE1.	Issue MODIFY *procname*,INOPDUMP=ON,TRLE=TRLE1.	*z/OS Communications Server: SNA Operation*
Re-create the InOp.	Take appropriate steps to re-create.	*z/OS Communications Server: SNA Operation*
Disable InOpDump.	Issue MODIFY *procname*,INOPDUMP=OFF.	*z/OS Communications Server: SNA Operation*
Restore InOpCode defaults.	Issue MODIFY *procname*,INOPCODE=(ALL,ALL,DUMPDEFAULT).	*z/OS Communications Server: SNA Operation*

IBM @server zSeries 990 HiperSockets enhancements

In z/OS V1R5 Communications Server, the following HiperSockets enhancements are available with and exclusive to the IBM @server zSeries 990:

- Spanned channels
- Increased number of HiperSockets CHPIDs (iQDIO Internal LANs)

  The number of Internal LANs that can be configured is increased from 4 to 16.
- Increased number of supported TCP/IP stacks

  The number of supported TCP/IP stacks is increased from 1024 to 4096.

iQDIO STAFD codes support this function. The first three were introduced in z/OS V1R2 Communications Server. The last three are new in z/OS V1R5 Communications Server:

- X'0065' iQDIO Activation Prohibited
- X'0066' iQDIO CHPID Ambiguous
- X'0067' iQDIO Subchannel Devices Not Available
- X'0068' iQDIO CHPID conflicts with sysplex IQDCHPID
- X'0069' iQDIO processor is not IQD capable
- X'006A' processor is MCSS capable but internal CHID is not available

Refer to *z/OS Communications Server: IP and SNA Codes* for complete information on these new codes.

Refer to *z/OS Communications Server: New Function Summary* for more information, including migration considerations regarding spanning. Refer to *z/OS Communications Server: IP Configuration Guide* for an overview of the concepts and considerations for IQD CHPIDs. Refer to *z/OS HCD User's Guide* for configuration details.

Network management

A new management interface is provided to allow network management applications to obtain real-time information, programmatically, from VTAM. The information provided by this interfaces includes:

- Enterprise Extender and High Performance Routing (HPR) connectivity and performance data
- Global CSM buffer statistics

This new interface is disabled by default and must be enabled using the SNAMGMT start option. Documentation on these programming interfaces can be found in *z/OS Communications Server: IP Programmer's Reference*.

Note: APARs PQ77244, PQ77837, PQ77838, and PQ77840 provide the ability to collect network management information using Network Management Interface APIs in z/OS V1R4.

Restrictions

The client application must reside on the same z/OS image as the VTAM address space.

Dependencies

An AF_UNIX NETWORK statement must be configured in the BPXPRM*xx* parmlib member.

What this change affects

- Application development
- Operations
- Performance

Using this function

The network management enhancements do not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 164. Network management

Task	Procedure	Reference

Define the AF_UNIX socket domain (only necessary if AF_UNIX socket is not already defined).
 	
Use the DISPLAY OMVS,PFS command to determine whether the AF_UNIX socket domain is already defined.
	Add the following to the BPXPRMxx parmlib member:
	`FILESYSTYPE TYPE(UDS)`
	`ENTRYPOINT(BPXTUINT)`
	`  NETWORK`
	`  DOMAINNAME(AF_UNIX)`
	`  DOMAINNUMBER(1) MAXSOCKETS(nnn)`
	`  TYPE(UDS)`
	
	where *nnn* is the maximum number of AF_UNIX sockets you expect to have open at any one time.
		z/OS UNIX System Services Planning

Define an OMVS segment for VTAM (only necessary if an OMVS segment is not already defined). The VTAM OMVS user ID must have write access to /var directory (the default for z/OS installation is write access to the /var directory.)	Issue the following commands: 1. ADDUSER vtamprocname OMVS(UID*(uid)* HOME('/') PROGRAM('/bin/sh')) Where *uid* is the UID you choose for the VTAM address space user ID. 2. RDEFINE STARTED vtamprocname.* STDATA(USER(vtamprocname)) 3. SETROPTS RACLIST(STARTED) REFRESH	*z/OS Communications Server: SNA Resource Definition Reference*, *z/OS Security Server RACF Command Language Reference*, and *z/OS UNIX System Services Planning*
Enable the service to VTAM.	Specify the VTAM start option SNAMGMT=YES in the VTAM Start List or on the START command for VTAM, or issue MODIFY VTAMOPTS,SNAMGMT=YES after VTAM is started.	*z/OS Communications Server: SNA Resource Definition Reference*, *z/OS Communications Server: SNA Operation*, and *z/OS Communications Server: Quick Reference*
Verify the status of the interface setting	Issue the following command: DISPLAY NET,VTAMOPTS.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: Quick Reference*

Table 164. Network management (continued)

Task	Procedure	Reference
Once this interface is enabled, by default, only applications that have superuser authority (access to BPX.SUPERUSER) or applications with a UID of 0 will be permitted access to this interface. You can further limit access to this service to specific applications through the use of RACF (or an equivalent external security manager).	Issue the following commands: 1. SETROPTS CLASSACT(SERVAUTH) 2. SETROPTS RACLIST(SERVAUTH) 3. RDEFINE SERVAUTH IST.NETMGMT.sysname.SNAMGMT UACC(NONE) 4. PERMIT IST.NETMGMT.sysname.SNAMGMT CLASS(SERVAUTH) ID(*userid*) ACCESS(READ) Where *userid* is the client's user ID that is to be permitted. 5. SETROPTS RACLIST(SERVAUTH) REFRESH	*z/OS Communications Server: SNA Resource Definition Reference* and *z/OS Security Server RACF Command Language Reference*
Disable the interface to VTAM when it is currently enabled.	Issue MODIFY VTAMOPTS,SNAMGMT=NO.	*z/OS Communications Server: SNA Operation*

Chapter 9. V1R4 SNA new function summary

This chapter includes a section for every function or enhancement introduced for SNA in z/OS V1R4 Communications Server. The sections include the following 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. The tables include references to the documents that contain more detailed information for each task.

See Table 125 on page 177 for a complete list of the SNA functional enhancements of the current and recent releases.

Refer to *z/OS Migration* for information about how to maintain the functional behavior of previous releases. Refer to *z/OS Summary of Message and Interface Changes* for information on new and changed messages and interfaces.

CSALIMIT start option behavioral change

z/OS V1R4 Communications Server changes the behavior of the CSALIMIT start option. Prior to z/OS V1R4 Communications Server, if a value was specified for the CSALIMIT start option and that value was reached, VTAM might have stopped executing. With z/OS V1R4 Communications Server, VTAM now continues executing beyond the value specified for CSALIMIT if sufficient CSA and ECSA storage is available. This might preclude the need to restart VTAM when the specified CSALIMIT is reached.

The ability to specify the ,F modifier has been extended to the CSALIMIT start option. It was previously only applicable to the MODIFY CSALIMIT and MODIFY VTAMOPTS,CSALIMIT commands. Refer to *z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Resource Definition Reference*.

Changed sample display, some new messages, and a changed message are associated with this enhancement. For example, if a programmed operator receives the output of a display BFRUSE command message group, a new message is added. If a programmed operator receives console output, two new messages are added.

Restrictions

None.

What this change affects

- Availability
- Usability
- Storage

Using this function

If you want VTAM to continue executing beyond the value specified for CSALIMIT if sufficient CSA and ECSA storage is available, you do not need to take any action. With z/OS V1R4 Communications Server, that is the default behavior of CSALIMIT. If, however, you want a value currently coded for the CSALIMIT start option to execute exactly as it has in the past, a new CSALIMIT start option modifier may be required. If that is the case, then perform the task in the following table.

Table 165. CSALIMIT start option behavioral change

Task	Procedure	Reference
If you want the CSALIMIT start option to behave as it did in prior releases, use a new command modifier.	Add a comma F after the value. For example, CSALIMIT=(value,F).	*z/OS Communications Server: SNA Resource Definition Reference*

Enterprise Extender dial processing enhancements

z/OS V1R4 Communications Server enhances the dial processing for Enterprise Extender connections to attempt automatic redial both in the case where an initial dial fails and in the case where an existing connection fails. Prior to z/OS V1R4 Communications Server, there was no mechanism to automatically attempt to redial a switched Physical Unit for Enterprise Extender when a dial attempt failed or when an existing connection INOPed.

Restrictions

None.

What this change affects

- Usability
- Operations

Using this function

The dial processing enhancements involve the tasks in Table 166 on page 233. Perform the tasks of your choice.

Usage Note: When VARY HANGUP is issued for an Enterprise Extender connection, it causes a connection INOP on the remote host. Therefore, if DWINOP=YES is coded on the switched PU on the remote host, the remote host will attempt to re-establish the connection by dialing back to the host that issued the VARY HANGUP. If the VARY HANGUP command successfully placed the switched PU in connectable state on this host, then that dial attempt will succeed. (See the next-to-last step in the following table.) If you want to prevent connection re-establishment when DWINOP is coded on the switched PU definition on the remote host, then perform the last step in the following table.

Table 166. Enterprise Extender dial processing enhancements

Task	Procedure	Reference
Enable XCA Enterprise Extender line to be automatically reactivated after link INOP.	No action is required; in z/OS V1R4 Communications Server, this is the default behavior (the default is KEEPACT=YES). If you wish to code it anyway, code the new KEEPACT operand on the GROUP or LINE statement in the XCA major node used for Enterprise Extender as KEEPACT=YES.	*z/OS Communications Server: SNA Resource Definition Reference*
Keep the behavior of past releases and disallow the XCA Enterprise Extender line to be automatically reactivated after link INOP.	Code KEEPACT=NO on the GROUP or LINE statement in the XCA major node used for Enterprise Extender if you do *not* want VTAM to attempt to automatically reactivate the line.	*z/OS Communications Server: SNA Resource Definition Reference*
Enable the switched PU used for Enterprise Extender to be automatically redialed *after a dial failure*, and specify how often to attempt to redial and for how long.	Code the new REDDELAY operand on the PATH statement to specify how long to wait after the dial failure before attempting a redial. Code the existing REDIAL operand on the PATH statement to a value in the range of 1 - 254 to specify a limited number of redial attempts, or code it to FOREVER to specify an unlimited number of redial attempts.	*z/OS Communications Server: SNA Resource Definition Reference*
Enable the switched PU used for Enterprise Extender to be automatically redialed *after failure of an existing connection*, and specify how often to attempt redial and for how long.	Code the new DWINOP operand on the PU statement in the switched major node as DWINOP=YES. Code REDIAL and REDDELAY on the PATH statement as described in the preceding procedure.	*z/OS Communications Server: SNA Resource Definition Reference*
Allow connection re-establishment when DWINOP is coded on the switched PU definition on the remote host.	Code either CALL=IN or CALL=INOUT on the Enterprise Extender PATH statement, and code ANSWER=ON on GROUP statement in the XCA major node to which the PATH statement applies.	*z/OS Communications Server: SNA Resource Definition Reference*
Break the connection and prevent connection re-establishment when DWINOP is coded on the switched PU definition on the remote host.	Do one of the following: • Code either CALL=OUT on the Enterprise Extender PATH statement or ANSWER=OFF on GROUP statement in the XCA major node to which the PATH statement applies, then issue the VARY NET HANGUP command. • Issue the VARY NET INACT command for the switched PU.	*z/OS Communications Server: SNA Resource Definition Reference*

Enterprise Extender addressing enhancement for logical lines and PUs

z/OS V1R4 Communications Server enhances the addressing for Enterprise Extender's logical lines and physical units (PUs) by making their assigned element addresses into extended element addresses. This is reflected in the displays seen with messages IST1863I and IST1864I in response to a DISPLAY VTAMSTOR, RESOURCE or a DISPLAY VTAMSTOR,NETADDR command.

The enhancement alleviates the constraint of network addresses for Enterprise Extender by expanding the network address allocations above and beyond the 64K line, up to 16M.

Restrictions

The number of available element address for Enterprise Extender's logical lines and PUs are still subject to a limit, although the limit has been raised up to 16M.

What this change affects

- APPN
- Scalability

Using this function

The Enterprise Extender addressing enhancement for logical lines and PUs function does not require any action; it is automatically enabled.

Enable HPR-only VRNs for interchange sessions

Prior to z/OS V1R4 Communications Server, you could not configure Interchange Nodes (ICNs) with links to some types of connection networks (such as ATM and Enterprise Extender connection networks) due to a configuration restriction that did not allow ICNs to exploit HPR over connection networks for sessions that cross from APPN into subarea. (ICNs could compute session paths through these connection networks for other APPN NNs or ENs that have links to them. However, the ICNs themselves could not activate a link to these types of connection networks. Instead, ICNs were required to predefine links to all other nodes on the connection network, or allow APPN to compute session paths that include additional nodes.)

z/OS V1R4 Communications Server eliminates this restriction for Enterprise Extender connection networks. In addition, this function will also allow HPR to be used (instead of ISR) over other types of connection networks (like token-ring) for sessions that cross from APPN into subarea.

Restrictions

This function does not support Interchange Nodes defining and activating links to ATM connection networks.

Incompatibilities

If Interchange Nodes attempt to define and activate links to Enterprise Extender connection networks when one or more VTAM Network Nodes in the network are running pre-z/OS V1R2 Communications Server, then sessions may fail intermittently with sense code x'08400002'.

Dependencies

In order to define and activate links to Enterprise Extender connection networks at Interchange Nodes, all VTAM Network Nodes in that APPN network must be running z/OS V1R2 Communications Server or above. In addition, both the Interchange Node and the node on the other side of the connection network (if it is a VTAM node) must be running z/OS V1R4 or above.

What this change affects

- Usability
- Availability
- Connectivity

Using this function

No start option changes are required to enable this enhancement; however, you do need to perform the tasks in the following table. **Perform the migration tasks in the order listed.**

Table 167. Enable HPR-only VRNs for interchange sessions

Task	Procedure	Reference
Ensure that all VTAM NNs and ICNs in the network are running at z/OS V1R2 Communications Server or a later release.	Determine the release you are running by issuing the DISPLAY VTAMOPTS command.	*z/OS Communications Server: SNA Operation*
Ensure that all VTAM NNs, ICNs, ENs, and MDHs that define connections to the same EE connection network as other ICNs are running at z/OS V1R4 Communications Server or a later release.	Determine the release you are running by issuing the DISPLAY VTAMOPTS command.	*z/OS Communications Server: SNA Operation*
After you have completed the first two tasks in this table, define and activate the link to the EE connection network at ICNs.	Define an XCA major node with MEDIUM=HPRIP and VNNAME.	*z/OS Communications Server: SNA Resource Definition Reference*

Display ID=rtpname diagnostic enhancement

z/OS V1R4 Communications Server adds additional data to the display for an RTP physical unit for diagnostic purposes. The operator can control whether or not most of this additional data is displayed.

Restrictions

None.

What this change affects

- Usability
- Diagnosis
- Serviceability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 168. Additional diagnostic data for Display ID=rtpname

Task	Procedure	Reference
View the base diagnostic and performance information for an RTP physical unit, including the actual data flow rate and the number of sessions using this RTP.	Issue the DISPLAY ID=rtpname command.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*
View additional diagnostic and performance information for an RTP physical unit.	Issue the DISPLAY ID=rtpname,HPRDIAG=YES command.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*

SRB mode dump enhancement

When an error occurs, a dump may be scheduled as part of recovery processing. Sometimes the data to be dumped may have changed between the time the error occurred and the time the dump is actually taken. This loss of data may require you to re-create the problem in order to capture sufficient data to diagnose the problem.

z/OS V1R4 Communications Server improves dump processing when running in SRB mode. During recovery, if running in SRB mode, the dump process now suspends processing until the data has been captured. This prevents the loss of data during the dump process and therefore requires fewer re-creates. Furthermore, in some cases, both VTAM and TCP address spaces will be dumped, making the dump more useful.

Restrictions

None.

What this change affects

- Diagnosis
- Serviceability

Using this function

This enhancement does not require any action; it is automatically enabled.

Increase maximum value for AUTOGEN on XCA major nodes

z/OS V1R4 Communications Server increases the maximum value for the num_stmts parameter for the AUTOGEN operand on the XCA major node from 4096 (4K) to 65 536 (64K). This is useful because increasing the number of line and PU statements that may be generated for each GROUP in an XCA major node will allow you to use AUTOGEN to eliminate the definitional requirement of defining multiple GROUPs or predefining all line and PU names when more than 4096 EE connection partners exist.

Note: Using this function may significantly increase the amount of storage required if the number of lines and PUs generated is large. As a result, you may have to increase the VTAM region size.

Restrictions

For specifications of 4097 or higher, the maximum number of line and PU seed characters permitted will be four. Up to five seed characters will still be permitted for specifications of 4096 or less. For specifications of 4097 or higher, the CUA® will not be included in the generated names.

What this change affects

- Operations
- Usability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the task in the following table.

Table 169. Increase maximum value for AUTOGEN on XCA major nodes

Task	Procedure	Reference
Specify that between 4097 and 65 536 line and PU statements should be automatically generated for an XCA major node group.	On the GROUP statement for an XCA major node, specify AUTOGEN=(65535,XLIN,XPU), for example.	*z/OS Communications Server: SNA Resource Definition Reference*

VIT data timestamp enhancement

z/OS V1R4 Communications Server includes estimated timestamps for the VIT records extracted from both internal VITs (ECSA and data space) by the VTAMMAP VITAL dump formatting tool. These timestamps are approximated using times saved in VTAM internal control blocks and available at dump formatting time to VITAL. The actual timestamps contained in the dump record the times when certain landmark events occurred in writing the internal VIT records, such as the time that each VIT wrapped and the time that data from the ECSA VIT was last copied to the data space VIT.

This enhancement benefits you because approximated timestamps in the VITAL output, while not necessarily accurately representing the actual clock time when events occurred, can be used to specify, as input to the VIT Analysis tool, start and stop times for subsets of records that you might wish to extract to another data set. This was not possible prior to z/OS V1R4 Communications Server because all VIT records extracted by the VITAL function contained the same timestamp.

Restrictions

None.

What this change affects

- Diagnosis
- Usability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 170. Additional timestamp data requested in VIT data

Task	Procedure	Reference
Extract VIT records from the internal VITs (both ECSA and data space VITs) that contain approximated time stamps.	Invoke the VTAMMAP VITAL function under IPCS for a VTAM dump.	*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*

Table 170. Additional timestamp data requested in VIT data (continued)

Task	Procedure	Reference
Use the timestamps in the VITAL output obtained in the previous task to extract a subset of VIT records from the VITAL output based on start and stop times.	Perform the following steps: 1. Extract the desired VIT records of the problem to be solved by specifying one of the following as input to the VIT Analysis Tool: • A resource name • VIT options or entries • Address • Other hexadecimal or character string 2. Note the approximated timestamps on the entries thus obtained that correspond to the events in which you are interested. 3. Use those timestamps as input for the Start Time and Stop Time parameters when invoking the VIT Analysis Tool again to help identify the part of the VIT that corresponds to the time of the failure being analyzed.	*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*

VARY ACT,UPDATE command for CDRSC Major Nodes enhancement

z/OS V1R4 Communications Server enhances the VARY ACT,UPDATE command to allow specification of a CDRSC Major Node on the command. You can now update a CDRSC Major Node to add, modify, or delete a CDRSC without having to inactivate the entire Major Node, thereby eliminating the disruption of all existing sessions using the CDRSC resources under the node.

Restrictions

None.

What this change affects

- Availability
- Usability

Using this function

This enhancement does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 171. VARY ACT,UPDATE command for CDRSC Major Nodes enhancement

Task	Procedure	Reference
Add a CDRSC definition to an active CDRSC Major Node.	Perform the following steps: 1. Add the new CDRSC definition to the VTAMLST member for the active CDRSC Major Node. 2. Issue VARY NET,ACT,ID=cdrscmajnode,UPDATE=ADD or VARY NET,ACT,ID=cdrscmajnode,UPDATE=ALL.	*z/OS Communications Server: SNA Operation*

Table 171. VARY ACT,UPDATE command for CDRSC Major Nodes enhancement (continued)

Task	Procedure	Reference
Delete a CDRSC definition from an active CDRSC Major Node.	Perform the following steps: 1. Delete the CDRSC definition from the VTAMLST member for the active CDRSC Major Node. 2. Be sure that the CDRSC to be deleted is inactive (If DISPLAY NET,ID=cdrscname shows the CDRSC is active, issue VARY NET,INACT,ID=cdrscname). 3. Issue VARY NET,ACT,ID=cdrscmajnode,UPDATE=ALL. **Note:** Steps 1 and 2 can be done in reverse order.	*z/OS Communications Server: SNA Operation*
Modify a table name operand (ASLTAB, MDLTAB, or MODETAB) for a CDRSC definition in an active CDRSC Major node.	Perform the following steps: 1. Modify the desired table name operands on the CDRSC definition in the VTAMLST member for the active CDRSC Major Node. You do not have to inactivate the CDRSC being modified to change these operands. 2. Issue VARY NET,ACT,ID=cdrscmajnode,UPDATE=ALL.	*z/OS Communications Server: SNA Operation*
Modify any allowed operand other than a table name operand (ASLTAB, MDLTAB, or MODETAB) for a CDRSC definition in an active Major Node. Refer to the discussion on dynamic change of operands for the Cross-Domain resource (CDRSC) major node in *z/OS Communications Server: SNA Resource Definition Reference* for the list of allowed operands.	Perform the following steps: 1. Modify the desired operands on the CDRSC definition in the VTAMLST member for the active CDRSC Major Node. 2. Be sure that the CDRSC to be modified is inactive (If DISPLAY NET,ID=cdrscname shows the CDRSC is active, issue VARY NET,INACT,ID=cdrscname). 3. Issue VARY NET,ACT,ID=cdrscmajnode,UPDATE=ALL. **Note:** Steps 1 and 2 can be done in reverse order.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Resource Definition Reference*

OPEN Application Control Block (ACB) limit increase

z/OS V1R4 Communications Server increases application capacity through VTAM to a new limit of 1,044,480. Prior to z/OS V1R4 Communications Server, the limit was approximately 65K open ACBs at a time.

Restrictions

None.

What this change affects

- Application capacity

Using this function

This enhancement does not require any action; it is automatically enabled.

NQNMODE support for Directory Services (DS) database entries

Prior to z/OS V1R4 Communications Server, you could not predefine the real name of resources on a Network Node and have that name used for APPN searches from other nodes. The resource could be predefined as an APPN Cross-Domain Resource (CDRSC) to prime the Directory Services (DS) database by coding CPNAME= on the CDRSC, but DS did not have a concept of REAL versus ALIAS names. When DS received a locate request with an ALIAS name (non-authentic NETID), DS searched the database and returned the first name entry found, but when the search was forwarded it still indicated that the NETID was not authentic. This can cause search problems especially in multiple subnetwork environments, because the Extended Border Nodes will not use the proper adjacent cluster tables to control the searching of multiple subnetworks.

z/OS V1R4 Communications Server adds NQNMODE support to Directory Services (DS) by enhancing the existing predefined CDRSC process. When CPNAME= is coded on a CDRSC, the NQNMODE value will be passed to DS during CDRSC processing. When DS performs a database query, if a predefined entry is found then DS will use the predefined NETID for all search tasks and will set the NETID indicator to authentic.

z/OS V1R4 Communications Server also enhances the predefined CDRSC process to add NATIVE and SUBAREA operands to improve APPN and subarea search efficiency for predefined resources.

Restrictions

None.

What this change affects

- APPN
- Performance
- Usability

Using this function

The NQNMODE support for Directory Services (DS) database entries function does not require any action unless you want to take advantage of the function. If so, perform the tasks in the following table.

Table 172. NQNMODE support for Directory Services (DS) database entries

Task	Procedure	Reference
Predefine the real name of a resource on a network node so that served end nodes can utilize the definition.	Code CDRSC with CPNAME= on the network node. If necessary, also code NQNMODE=NAME on the network node. (Coding NQNMODE=NAME is not required on the CDRSC entry if it is already specified on the NQNMODE start option or on a preceding GROUP statement in the CDRSC major node.)	*z/OS Communications Server: SNA Resource Definition Reference*
Improve APPN and subarea search efficiency.	Code the new NATIVE and SUBAREA operands on CDRSC on the network node or end nodes.	*z/OS Communications Server: SNA Resource Definition Reference*

Changes to installing dump analysis and trace analysis tools

Prior to z/OS V1R4 Communications Server, you had to compile help panels, tables, keylists, and commands for the dump analysis and trace analysis tools. In z/OS V1R4 Communications Server, these items are shipped compiled. You will notice these changes in the installation procedure and in the shortened help panels.

Changes to PF key settings

Your previously-set PF keys will be restored to their prior settings upon exiting the following panels:

- VTAMMAP Analysis Menu
- VTAM Internal Trace Analysis

Changes in distribution libraries and parts

The following parts were deleted in z/OS V1R4 Communications Server:

- ISTDHELP
- ISTTHELP
- ISTDTABL
- ISTTTABL
- ISTDFIX
- ISTTFIX
- ISTTH16
- ISTTT026

The following libraries were deleted in z/OS V1R4 Communications Server:

- AISTCLI0
- AISTCLS1
- AISTMSG0
- AISTPNL0
- AISTPNL1
- SISTCLI0
- SISTCLS1
- SISTMSG0
- SISTPNL0
- SISTPNL1

The following parts were moved in distribution libraries in z/OS V1R4 Communications Server:

- ISTDE01
- ISTTE01
- ISTDH*
- ISTTH*
- ISTDT*
- ISTTT*
- ISTDKEYS
- ISTTKEYS
- ISTDCMDS
- ISTTCMDS

The following REXX EXECs now create tables of the same name:

- ISTDT020 now creates table ISTDT020.
- ISTDT025 now creates table ISTDT025.
- ISTDT033 now creates table ISTDT033.
- ISTDT037 now creates table ISTDT037.

- ISTDT053 now creates table ISTDT053.
- ISTTT007 now creates table ISTTT007.
- ISTTT010 now creates table ISTTT010.
- ISTTT012 now creates table ISTTT012.
- ISTTT017 now creates table ISTTT017.
- ISTTT024 now creates table ISTTT024.

Restrictions

None.

What this change affects

- Installation

Using this function

Be aware that you no longer have to compile help panels, tables, keylists, and commands for the dump analysis and trace analysis tools.

APPN topology traces enhancements

Traces are added to provide a record of the creation, update, and deletion of TRS (Topology and Routing Services) topology records.

There are three locations where topology tracing is done:

- In an NDREC (node record) trace table following the NDREC control block, where the creation and update of a node record is recorded.
- In a TGREC (TG record) trace table following the TGREC control block, where the creation and update of a TG record is recorded.
- In a common TRS (Topology and Routing Services) trace table, where the deletion of NDRECs and TGRECs are recorded.

Users of APPN will notice an increase in storage utilization because VTAM will now allocate an additional one to ten 4K pages for the table of topology deletions, 110 bytes per node record for the NDREC traces, and 180 bytes per TG record for the TGREC traces.

Note: Enhancements to APPN topology traces will be available for z/OS V1R2 Communications Server and will be documented by FIN APAR OW51867.

Restrictions

None.

What this change affects

- Serviceability

Using this function

There are no migration procedures; this function is automatic for z/OS V1R4 Communications Server.

VTAM IPCS CLIST changes

The VTAM IPCS CLIST ISTVMAP was changed by APAR OW51239 so that there is a new ASID parameter, and that new ASID is now the default. The VTAM IPCS CLIST ISTVMAP maps the storage for an address space. Previously, the only ASID the CLIST used was VTAM's. Now, with this APAR, the VTAM ASID is selected only if three other tests fail. This CLIST can now be used with any ASID, not just VTAM's.

The ASID search order is as follows:

- The ASID parameter value
- The default ASID, if set
- ASID from dump header
- VTAM's ASID
- 001

The first match found in the list above is used.

The ASID of the address space to be mapped may be entered when the CLIST is invoked. The ASID may be specified in decimal or in hexadecimal by using the format X'nn'. For example, to invoke the ISTVMAP CLIST to produce a storage map for ASID X'1B', you could invoke the CLIST in one of the following ways (Note: X'1B' is equal to 27 decimal):

```
ISTVMAP ASID(X'1B')
```

or

```
ISTVMAP ASID(27)
```

If no ASID is specified, the current ASID will be used. The current ASID is the one that was specified in the IPCS SETDEF command. If that ASID cannot be determined, the ASID from the dump header will be used (the ASID that was current when the dump was taken.

Note: If the dump contains multiple address spaces, this ASID will be 0001. If the ASID cannot be obtained from the dump header, VTAM's ASID will be used. If VTAM's ASID cannot be determined, ASID 0001 will be used.

Prior to APAR OW51239, VTAM's ASID was used to produce the storage map. If VTAM's ASID was not dumped, some of the storage ranges would not be available. APAR OW51239 changed the ISTVMAP CLIST to use an ASID that would produce more meaningful results for the dump being processed.

Restrictions

None.

Using this function

The VTAM IPCS CLIST changes do not require any action if you want to use the new default ASID parameter. If you want to keep the pre-V1R4 behavior, perform the task in the following table:

Table 173. VTAM IPCS CLIST changes - task to keep pre-V1R4 behavior

Task	Procedure	Reference
Use VTAM's ASID (keep the pre-V1R4 behavior for the VTAM IPCS CLIST ISTVMAP).	Code ISTVMAP ASID(*asid*) where *asid* is the VTAM's ASID.	*z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*

VTAM INOPDUMP enhancement

In z/OS V1R4 Communications Server, VTAM INOPDUMP is enhanced to more granularly control which resources are affected by the function. This is done by allowing the function to be activated or inactivated based on a transport resource list entry (TRLE). For example, INOPDUMP can now be generally inactive, yet active for a specific TRLE. This prevents dumps from being taken when inoperative conditions occur on links other than those targeted by this function.

The MODIFY INOPDUMP command can be used to alter the TRLE InOpDump status for TRLEs that are not active, as long as that TRLE is contained in the TRL major node. The status will be saved and put into effect when the TRLE becomes active.

Identification of additional normal inoperative conditions has resulted in the internal suppression of INOPDUMP for these conditions.

Prior to z/OS V1R4 Communications Server, the VTAM INOPDUMP function had an all-or-nothing operation. This enhancement is a serviceability benefit because it reduces the impact of gathering documentation for an inoperative condition.

Restrictions

Resources not defined within a transport resource list entry cannot be individually controlled. However, the TRLE resources can be excluded from global INOPDUMP control by using the new support to specifically set INOPDUMP off for each active TRLE.

Incompatibilities

Prior to z/OS V1R4 Communications Server, the INOPDUMP function is controlled using the INOPDUMP start option. The INOPDUMP start option is displayable and modifiable by specifying INOPDUMP as the option on the DISPLAY VTAMOPTS and MODIFY VTAMOPTS commands. In z/OS V1R4 Communications Server, there are new DISPLAY INOPDUMP and MODIFY INOPDUMP commands which also allow you to display and modify the INOPDUMP setting. Display and modification of INOPDUMP is still supported through the DISPLAY VTAMOPTS and MODIFY VTAMOPTS commands, and that mechanism is functionally equivalent to the new method. Both methods set or reset INOPDUMP globally and for each TRLE in the TRL major node.

The responses to the modify commands will differ primarily when the TRL major node is unavailable. If the TRL major node is unavailable, the MODIFY INOPDUMP response will include IST1865I (GLOBAL INOPDUMP = xxx), while the MODIFY VTAMOPTS variation will provide the same response as previous releases. The MODIFY VTAMOPTS variation ends its response with IST223I MODIFY COMMAND COMPLETED, while the MODIFY INOPDUMP response ends with IST223I MODIFY INOPDUMP COMMAND COMPLETED.

The responses to the two display commands will be significantly different. The response to the DISPLAY VTAMOPTS,OPTION=INOPDUMP command will not change. The response to the DISPLAY INOPDUMP command will include IST097I, IST350I, IST1865I, possibly some number of 1866I messages, and IST314I.

Using this function

If you want to use the VTAM INOPDUMP enhancement, perform the desired tasks in the following table:

Table 174. VTAM INOPDUMP enhancement

Task	Procedure	Reference
If you need InOpDump for problem analysis, issue the Modify InOpDump command against the trlename for which a dump is to be taken.	Issue MODIFY procname,INOPDUMP=ON,TRLE=trlename.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*
Re-create the inoperative condition.	Repeat the steps that lead up to the initial inoperative condition. A dump should be taken. Save the dump for VTAM service.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*
Reset InOpDump for the TRLE to prevent VTAM from taking additional dumps.	Issue MODIFY procname,INOPDUMP=OFF,TRLE=trlename or MODIFY procname,INOPDUMP=OFF.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*
Determine the status of either global InOpDump or individual TRLE InOpDump.	Issue DISPLAY NET,INOPDUMP or DISPLAY NET,ID=trlename or DISPLAY NET,TRL,TRLE=trlename.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*
Reset or set global InOpDump and all TRLE InOpDump status with a single command.	Issue MODIFY procname,INOPDUMP=ON|OFF or MODIFY procname,VTAMOPTS,INOPDUMP=ON|OFF.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*
Determine the status of global InOpDump. Note that this will not show TRLE InOpDump status.	Issue DISPLAY NET,VTAMOPTS or DISPLAY NET,VTAMOPTS,OPT=INOPDUMP or DISPLAY NET,VTAMOPTS,FUNCTION=ZAPCON or DISPLAY NET,VTAMOPTS,FUNCTION=TRACDUMP.	*z/OS Communications Server: SNA Operation* and *z/OS Communications Server: SNA Messages*

New start options to adjust the QDIO or iQDIO storage

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

OSA–Express storage for read processing

Table 175. OSA–Express: Amount of storage for read processing

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

HiperSockets storage for read processing

Table 176. HiperSockets: Amount of storage for read processing

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

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

The new options are as follows:

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

The iQDIO MFS is defined in HCD. The storage units are defined in QDIO SBALs (QDIO read buffers). Each SBAL is 64k. The storage used for this read processing is allocated from CSM data space 4k pool, and is fixed storage.

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

Restrictions

None.

Using this function

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

Table 177. New start options to adjust the QDIO or iQDIO storage

Task	Procedure	Reference
Recommended: Review CSM specifications for fixed CSM storage.	Review (and alter if necessary) the IVTPRM00 parmlib member for CSM fixed storage.	Refer to *z/OS MVS Initialization and Tuning Reference* and refer to *SNA Resource Definition Reference* Information APAR ii13235 for additional CSM information.

Table 177. New start options to adjust the QDIO or iQDIO storage (continued)

Task	Procedure	Reference
Optionally: Define how much storage VTAM keeps available for read processing for all OSA QDIO data devices.	Code the QDIOSTG (QDIO Storage) start option.	*SNA Resource Definition Reference* Information APAR ii13235
Optionally: Define how much storage VTAM keeps available for read processing for all HiperSockets (iQDIO) data devices that use a MFS (Maximum Frame Size) of 64k.	Code the IQDIOSTG (iQDIO Storage) start option.	*SNA Resource Definition Reference* Information APAR ii13235

Part 4. Appendixes

Appendix A. Related protocol specifications (RFCs)

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

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 260 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
768	*User Datagram Protocol* J. Postel
791	*Internet Protocol* J. Postel
792	*Internet Control Message Protocol* J. Postel
793	*Transmission Control Protocol* J. Postel
821	*Simple Mail Transfer Protocol* J. Postel
822	*Standard for the Format of ARPA Internet Text Messages* D. Crocker
823	*DARPA Internet Gateway* R. Hinden, A. Sheltzer
826	*Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.Bit Ethernet Address for Transmission on Ethernet Hardware* D. Plummer
854	*Telnet Protocol Specification* J. Postel, J. Reynolds
855	*Telnet Option Specification* J. Postel, J. Reynolds
856	*Telnet Binary Transmission* J. Postel, J. Reynolds

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

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

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

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

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

862 *Echo Protocol* J. Postel

863 *Discard Protocol* J. Postel

864 *Character Generator Protocol* J. Postel

877 *Standard for the Transmission of IP Datagrams over Public Data Networks* J. Korb

885 *Telnet End of Record Option* J. Postel

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

896 *Congestion Control in IP/TCP Internetworks* J. Nagle

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

904 *Exterior Gateway Protocol Formal Specification* D. Mills

919 *Broadcasting Internet Datagrams* J. Mogul

922 *Broadcasting Internet Datagrams in the Presence of Subnets* J. Mogul

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

951 *Bootstrap Protocol* W.J.Croft, J.Gilmore

952 *DoD Internet Host Table Specification* K. Harrenstien, M. Stahl, E. Feinler

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

974 *Mail Routing and the Domain Name System* C. Partridge

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

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

1006 *ISO Transport Service on top of the TCP Version 3* M. Rose, D. Cass

1009 *Requirements for Internet Gateways* R. Braden, J. Postel

1011 *Official Internet Protocols* J. Reynolds, J. Postel

1013 *X Window System Protocol, Version 11: Alpha Update* R. Scheifler

1014 *XDR: External Data Representation Standard* Sun Microsystems Incorporated

1027 *Using ARP to Implement Transparent Subnet Gateways* S. Carl-Mitchell, J. Quarterman

1032 *Domain Administrators Guide* M. Stahl

1033 *Domain Administrators Operations Guide* M. Lottor

1034 *Domain Names—Concepts and Facilities* P. Mockapetris

1035 *Domain Names—Implementation and Specification* P. Mockapetris

1042 *Standard for the Transmission of IP Datagrams over IEEE 802 Networks* J. Postel, J. Reynolds

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

1055 *Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP* J. Romkey

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

1058 *Routing Information Protocol* C. Hedrick

1060 *Assigned Numbers* J. Reynolds, J. Postel

1073 *Telnet Window Size Option* D. Waitzman

1079 *Telnet Terminal Speed Option* C. Hedrick

1091 *Telnet Terminal-Type Option* J. VanBokkelen

1094 *NFS: Network File System Protocol Specification* Sun Microsystems Incorporated

1096 *Telnet X Display Location Option* G. Marcy

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

1112 *Host Extensions for IP Multicasting* S. Deering

1118 *Hitchhikers Guide to the Internet* E. Krol

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

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

1155 *Structure and Identification of Management Information for TCP/IP-Based Internets* M. Rose, K. McCloghrie

1156 *Management Information Base for Network Management of TCP/IP-Based Internets* K. McCloghrie, M. Rose

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

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

1179 *Line Printer Daemon Protocol* The Wollongong Group, L. McLaughlin III

1180 *TCP/IP Tutorial* T. Socolofsky, C. Kale

1183 *New DNS RR Definitions* C. Everhart, L. Mamakos, R. Ullmann, P. Mockapetris, (Updates RFC 1034, RFC 1035)

1184 *Telnet Linemode Option* D. Borman

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

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

1191 *Path MTU Discovery* J. Mogul, S. Deering

1198 *FYI on the X Window System* R. Scheifler

1207 *FYI on Questions and Answers: Answers to Commonly Asked "Experienced Internet User" Questions* G. Malkin, A. Marine, J. Reynolds

1208 *Glossary of Networking Terms* O. Jacobsen, D.Lynch

1213 *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II* K. McCloghrie, M. Rose

1215 *Convention for Defining Traps for Use with the SNMP* M. Rose

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

1229 *Extensions to the Generic-Interface MIB* K. McCloghrie

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

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

1236 *IP to X.121 Address Mapping for DDN* L. Morales, P. Hasse

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

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

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

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

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

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

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

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

1348 *DNS NSAP RRs* B. Manning

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

1350 *TFTP Protocol* K.R. Sollins

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

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

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

1354 *IP Forwarding Table MIB* F. Baker

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

1363 *A Proposed Flow Specification* C. Partridge

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

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

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

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

1387 *RIP Version 2 Protocol Analysis* G. Malkin

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

1389 *RIP Version 2 MIB Extension* G. Malkin

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

1393 *Traceroute Using an IP Option* G. Malkin

1397 *Default Route Advertisement In BGP2 And BGP3 Versions of the Border Gateway Protocol* D. Haskin

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

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

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

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

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

1497 *BOOTP Vendeor Information Extensions* J.Reynolds

1533 *DHCP Options and BOOTP Vendor Extensions* S.Alexander, R.Droms

1534 *Interoperation Between DHCP and BOOTP* R.Droms

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

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

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

1540 *IAB Official Protocol Standards* J. Postel

1541 *Dynamic Host Configuration Protocol* R.Droms

1542 *Clarifications and Extensions for the Bootstrap Protocol* W.Wimer

1571 *Telnet Environment Option Interoperability Issues* D. Borman

1572 *Telnet Environment Option* S. Alexander

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

1583 *OSPF Version 2* J. Moy

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

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

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

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

1647 *TN3270 Enhancement* B.Kelly

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

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

1713 *Tools for DNS debugging* A. Romao

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

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

1794 *DNS Support for Load Balancing* T. Brisco

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

1840 *Schema Publishing in X500 Directory* G.Mansfield, P.Rajeev, S.Raghavan, T.Howes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1995 *Incremental Zone Transfer in DNS* M. Ohta

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

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

2011 *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2* K. McCloghrie

2012 *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2* K. McCloghrie

2013 *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2* K. McCloghrie

2030 *Simple Network Time Protocol* D. Mills

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

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

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

2096 *IP Forwarding Table MIB* F. Baker

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

2132 *DHCP Options and BOOTP Vendor Extensions* S. Alexander, R. Droms

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

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

2137 *Secure Domain Name System Dynamic Update* D. Eastlake

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

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

2178 *OSPF Version 2* J. Moy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2320 *Definitions of Managed Objects for Classical IP and ARP over ATM Using SMIv2* M. Greene, J. Luciani, K. White, T. Kuo

2328 *OSPF Version 2* J. Moy

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

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

2355 *TN3270 Enhancements* B. Kelly

2373 *IP Version 6 Addressing Architecture* R. Hinden, M. O'Dell, S. Deering

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

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

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

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

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

2403 *HMAC-MD5–96 within ESP and AH* Madson, R.Glenn

2404 *The Use of HMAC-MD5–96 within ESP and AH* C. Madson, R.Glenn

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

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

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

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

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

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

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

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

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

2474 *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* K. Nichols, S. Blake, F. Baker, D. Black

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

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

2535 *Domain Name System Security Extensions* D. Eastlake

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

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

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

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

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

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

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

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

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

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

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

2665 *Definitions of Managed Objects for the Ethernet-like Interface Types* J. Flick, J. Johnson

2672 *Non-Terminal DNS Name Redirection* M. Crawford

2710 *Multicast Listener Discovery (MLD) for IPv6*S. Deering, W. Fenner, B. Haberman

2711 *IPv6 Router Alert Option*C. Partridge, A. Jackson

2740 *OSPF for IPv6* R. Coltun, D. Ferguson, J. Moy

2758 *Definitions of Managed Objects for Service Level Agreements Performance Monitoring* K. White

2845 *Secret Key Transaction Authentication for DNS (TSIG)* P. Vixie, O. Gudmundsson, D. Eastlake, B. Wellington

2874 *DNS Extensions to Support IPv6 Address Aggregation and Renumbering* M. Crawford, C. Huitema

2941 *Telnet Authentication Option* T. Ts'o,, ed., J. Altman

2942 *Telnet Authentication: Kerberos Version 5* T. Ts'o

2946 *Telnet Data Encryption Option* T. Ts'o

2952 *Telnet Encryption: DES 64 bit Cipher Feedback* T. Ts'o

2953 *Telnet Encryption: DES 64 bit Output Feedback* T. Ts'o, ed.

3060 *Policy Core Information Model—Version 1 Specification* B. Moore, E. Ellesson, J. Strassner, A. Westerinen

3363 *Representing Internet Protocl version 6 (IPv6) Addresses in the Domain Name System* R.Bush, A.Durand, B.Fink, O.Gudmundsson,T.Hain

3390 *Increasing TCP's Initial Window* M. Allman, S. Floyd, C. Partridge

3411 *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*D.Harrington, R.Presuhn, B.Wijnen

3412 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*J.Case, D.Harrington, R.Presuhn, B.Wijnen

3413 *Simple Network Management Protocol (SNMP) Applications*D.Levi, P. Meyer, B.Stewart

3414 *User- Based Security Model (USM) for version 3 of the Simple Network management Protocol (SNMPv3)*U. Blumenthal, B. Wijnen

3415 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*B.Wijnen, R.Presuhn, K.McCloghrie

3484 *Default Address Selection for Internet Protocol version 6 (IPv6)* R. Draves

3493 *Basic Socket Interface Extensions for IPv6* R. Gilligan, S. Thomson, J. Bound, J. McCann, W. Stevens

3513 *Internet Protocol Version 6 (IPv6) Addressing Architecture* R. Hinden, S. Deering

3542 *Advanced Sockets API for IPv6* W. Richard Stevens, M. Thomas, E. Nordmark, T. Jinmei

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.

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 (GA27-3136-19)
- SNA Technical Overview (GC30-3073-04)

For more information, refer to the AIW documentation page at http://nhdidd.raleigh.ibm.com/app/aiwdoc.htm.

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. Information APARs

This appendix lists information APARs for IP and SNA documents.

Notes:

1. Information APARs contain updates to previous editions of the manuals listed below. Documents updated for V1R6 are complete except for the updates contained in the information APARs that might be issued after V1R6 documents went to press.
2. Information APARs are predefined for z/OS V1R6 Communications Server and might not contain updates.
3. Information APARs for z/OS documents are in the document called *z/OS and z/OS.e DOC APAR and PTF ++HOLD Documentation*, which can be found at http://publibz.boulder.ibm.com:80/cgi-bin/bookmgr_OS390/BOOKS/ZIDOCMST/CCONTENTS.

Information APARs for IP documents

Table 178 lists information APARs for IP documents.

Table 178. IP information APARs for z/OS Communications Server

Title	V1R6	V1R5	V1R4	V1R2
New Function Summary (both IP and SNA)	II13824			
Quick Reference (both IP and SNA)	II13831		II13246	II12500
IP and SNA Codes	II13842	II13576	II13254	II12504
IP API Guide	II13844	II13577	II13255 II13790	II12861 II13655
IP CICS Sockets Guide		II13578	II13257	II12862 II13627
IP Configuration Guide	II13826	II13568	II13244 II13541 II13652	II12498 II13087 II13364 II13634 II13651
IP Configuration Reference	II13827	II13569 II13789	II13245 II13521 II13647	II12499 II13394 II13637
IP Diagnosis	II13836	II13571	II13249 II13493	II12503 II13473
IP Messages Volume 1	II13838	II13572	II13624 II13250	II12857 II13229 II13405
IP Messages Volume 2	II13839	II13573	II13251	II12858
IP Messages Volume 3	II13840	II13574	II13252	II12859
IP Messages Volume 4	II13841	II13575	II13253 II13628	II12860
IP Migration		II13566	II13242 II13738	II12497 II13636

Table 178. IP information APARs for z/OS Communications Server (continued)

Title	V1R6	V1R5	V1R4	V1R2
IP Network and Application Design Guide	II13825	II13567	II13243	
IP Network Print Facility				II12864
IP Programmer's Reference	II13843	II13581	II13256	II12505
IP User's Guide				
IP User's Guide and Commands	II13832	II13570	II13247	II12501 II13404
IP System Admin Guide	II13833	II13580	II13248 II13792	II12502 II13793

Information APARs for SNA documents

Table 179 lists information APARs for SNA documents.

Table 179. SNA information APARs for z/OS Communications Server

Title	V1R6	V1R5	V1R4	V1R2
New Function Summary (both IP and SNA)	II13824			
Quick Reference (both IP and SNA)	II13831		II13246	II12500
IP and SNA Codes	II13842	II13576	II13254	II12504
SNA Customization	II13857	II13560	II13240	II12872
SNA Diagnosis		II13558	II13236	II12490 II13034
SNA Diagnosis, Vol. 1: Techniques and Procedures	II13852			
SNA Diagnosis, Vol. 2: FFST Dumps and the VIT	II13853			
SNA Messages	II13854	II13559	II13238	II12491
SNA Network Implementation Guide	II13849	II13555	II13234	II13635 II12487
SNA Operation	II13851	II13557	II13237	II12489
SNA Migration		II13554	II13233	II12486
SNA Programming	II13858		II13241	II13033
SNA Resource Definition Reference	II13850	II13556	II13235	II12488
SNA Data Areas		II13576	II13239	II12492
SNA Data Areas, 1	II13855			
SNA Data Areas, 2	II13856			

Other information APARs

Table 180 on page 265 lists information APARs not related to documents.

Table 180. Non-document information APARs

Content	Number
index of recommended maintenance for VTAM	II11220
index of Communication Server IP information APARs	II12028
AHHC, MPC, and CTC	II01501
Collecting TCPIP CTRACEs	II12014
CSM for VTAM	II12657
CSM for TCP/IP	II12658
DLUR/DLUS for z/OS V1R2	II12986
DOCUMENTATION REQUIRED FOR OSA/2, OSA EXPRESS AND OSA QDIO	II13016
DYNAMIC VIPA (BIND)	II13215
DNS — common problems and solutions	II13453
Enterprise Extender	II12223
FTPing doc to z/OS Support	II12030
FTP problems	II12079
Generic resources	II10986
HPR	II10953
iQDIO	II11220
LPR problems	II12022
MNPS	II10370
NCPROUTE problems	II12025
OMPROUTE	II12026
OROUTED problems	II12024
PASCAL API	II11814
Performance	II11710 II11711 II11712
Resolver	II13398 II13399 II13452
Socket API	II11996 II12020
SMTP problems	II12023
SNMP	II13477 II13478
SYSLOGD howto	II12021
TCPIP connection states	II12449
Telnet	II11574 II13135
TN3270 TELNET SSL common problems	II13369

Appendix D. Accessibility

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

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

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using 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 Volume I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer/Library Server versions of z/OS books in the Internet library at:

`www.ibm.com/servers/eserver/zseries/zos/bkserv/`

One exception is command syntax that is published in railroad track format; screen-readable copies of z/OS books with that syntax information are separately available in HTML zipped file form upon request to usib2hpd@vnet.ibm.com.

Notices

IBM may not offer all of the products, services, or features discussed in this document. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, North Carolina 27709-2195
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application

programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

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.

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.

Copyright © 1998 by the FundsXpress, INC. All rights reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of FundsXpress not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. FundsXpress makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright © 1999, 2000 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED ″AS IS″ AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

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

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

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be

given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following 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.

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

You can obtain softcopy from the z/OS Collection (SK3T-4269), which contains BookManager and PDF formats of unlicensed books and the z/OS Licensed Product Library (LK3T-4307), which contains BookManager and PDF formats of licensed books.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Advanced Peer-to-Peer Networking
AFP
AD/Cycle
AIX
AIX/ESA
AnyNet
APL2
AS/400
AT
BookManager
BookMaster
C/370
CICS
CICS/ESA
C/MVS
Common User Access
C Set ++
CT
CUA
DB2
DFSMSdfp
DFSMShsm
DFSMS/MVS
DPI
Domino
DRDA
Enterprise Systems Architecture/370
ESCON
eServer
ES/3090
ES/9000
ES/9370
EtherStreamer
Extended Services
FFST
FFST/2
First Failure Support Technology
GDDM
IBM
IBMLink
IMS
IMS/ESA
Java
HiperSockets
Language Environment
LANStreamer
Library Reader
LPDA
Micro Channel
Multiprise
MVS
MVS/DFP
MVS/ESA
MVS/SP
MVS/XA
NetView
Network Station
Nways
Notes
OfficeVision/MVS
OfficeVision/VM
Open Class
OpenEdition
OS/2
OS/390
OS/400
Parallel Sysplex
PR/SM
PROFS
PS/2
RACF
Redbooks
Resource Link
RETAIN
RISC System/6000
RMF
RS/6000
S/370
S/390
S/390 Parallel Enterprise Server
SAA
SecureWay
SP
SP2
SQL/DS
System/360
System/370
System/390
SystemView
Tivoli
TURBOWAYS
VM/ESA
VSE/ESA
VTAM
WebSphere
XT
z/Architecture
z/OS
zSeries
z/VM
400
3090
3890

DB2 and NetView are registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the U.S., other countries, or both.

The following terms are trademarks of other companies:

ATM is a trademark of Adobe Systems, Incorporated.

BSC is a trademark of BusiSoft Corporation.

CSA is a trademark of Canadian Standards Association.

DCE is a trademark of The Open Software Foundation.

HYPERchannel is a trademark of Network Systems Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both. For a complete list of Intel trademarks, see http://www.intel.com/sites/corporate/tradmarx.htm .

Other company, product, and service names may be trademarks or service marks of others.

Bibliography

z/OS Communications Server information

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

z/OS Communications Server documentation is available:

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

z/OS Communications Server library

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

Updates to documents are available on RETAIN and in information APARs (info APARs). See Appendix C, "Information APARs," on page 263 for a list of the documents and the info APARs associated with them.

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

Planning

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 • SMF records • 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: AnyNet SNA over TCP/IP	SC31-8832	This guide provides information to help you install, configure, use, and diagnose SNA over TCP/IP.
z/OS Communications Server: AnyNet Sockets over SNA	SC31-8831	This guide provides information to help you install, configure, use, and diagnose sockets over SNA. It also provides information to help you prepare application programs to use sockets over SNA.
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	LY43-0092	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 Application Programming Interface Guide	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 IBM's TCP/IP Services.
z/OS Communications Server: IP Programmer's 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: SNA Diagnosis Vol 1, Techniques and Procedures and *z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT*	LY43-0088 LY43-0089	These documents help you identify an SNA problem, classify it, and collect information about it before you call the IBM Support Center. The information collected includes traces, dumps, and other problem documentation.
z/OS Communications Server: SNA Data Areas Volume 1 and *z/OS Communications Server: SNA Data Areas Volume 2*	LY43-0090 LY43-0091	These documents describe SNA data areas and can be used to read an SNA dump. They are intended for IBM programming service representatives and customer personnel who are diagnosing problems with SNA.

Messages and codes

Title	Number	Description
z/OS Communications Server: SNA Messages	SC31-8790	This document describes the ELM, IKT, IST, ISU, 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)	SC31-8784	This volume contains TCP/IP messages beginning with EZB.
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.

APPC Application Suite

Title	Number	Description
z/OS Communications Server: APPC Application Suite User's Guide	SC31-8809	This documents the end-user interface (concepts, commands, and messages) for the AFTP, ANAME, and APING facilities of the APPC application suite. Although its primary audience is the end user, administrators and application programmers may also find it useful.

Title	Number	Description
z/OS Communications Server: APPC Application Suite Administration	SC31-8835	This document contains the information that administrators need to configure the APPC application suite and to manage the APING, ANAME, AFTP, and A3270 servers.
z/OS Communications Server: APPC Application Suite Programming	SC31-8834	This document provides the information application programmers need to add the functions of the AFTP and ANAME APIs to their application programs.

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+919-254-9823
- 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 and 5655–G52

Printed in USA

GC31-8771-00

Spine information:

z/OS Communications Server

z/OS V1R6.0 CS: New Function Summary

Version 1
Release 6