z/OS Communications Server 2.5

New Function Summary

GC27-3664-50

Note:

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 199.

This edition applies to Version 2 Release 5 of z/OS® (5650-ZOS), and to subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2023-06-26

Contents

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 2 Release 5 Communications Server (z/OS Communications Server). It also includes the exploitation considerations of z/OS V2R4 Communications Server.

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

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

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

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

Who should read this document

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

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

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

How this document is organized

This document contains these topics:

- Chapter 1, “Planning to use new functions,” on page 1 includes a brief introduction to z/OS Communications Server, information about hardware requirements, references to documents that will help you if you are migrating, information about the IP encryption features, a planning checklist, and data set information.
- Chapter 2, “Roadmap to functions,” on page 19 provides a roadmap of the functional enhancements introduced in z/OS V2R5 Communications Server and z/OS V2R4 Communications Server. Each entry indicates whether enabling actions are required.
- Chapter 3, “V2R5 new function summary,” on page 23 summarizes the functions and migration considerations of z/OS V2R5 Communications Server.
- Chapter 5, “V2R4 new function summary,” on page 99 summarizes the functions and migration considerations of z/OS V2R4 Communications Server.
- Appendix A, “Related protocol specifications,” on page 173 lists the related protocol specifications for TCP/IP.
- Appendix B, “Architectural specifications,” on page 193 lists documents that provide architectural specifications for the SNA Protocol.

- Appendix D, “Accessibility,” on page 197 describes accessibility features to help users with physical disabilities.
- “Notices” on page 199 contains notices and trademarks used in this document.
- “Bibliography” on page 203 contains descriptions of the documents in the z/OS Communications Server library.

How to use this document

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

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

Use the function summary topics to learn about this information:

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

How to provide feedback to IBM

We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information. See, How to send feedback to IBM for additional information.

Conventions and terminology that are used in this information

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

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

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

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

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

z/OS no longer supports mounting HFS data sets (The POSIX style file system). Instead, a z/OS File System (ZFS) can be implemented. The term hierarchical file system, abbreviated as HFS, is defined as a data structure that has a hierarchical nature with directories and files. References to hierarchical file systems or HFS might still be in use in z/OS Communications Server publications.

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

- RoCE Express®, which is a generic term representing IBM® 10 GbE RoCE Express, IBM 10 GbE RoCE Express2, IBM 25 GbE RoCE Express2, IBM 10 GbE RoCE Express3, and IBM 25 GbE RoCE Express3 feature capabilities. When this term is used in this information, the processing being described applies

to all of these features. If processing is applicable to only one feature, the full terminology, for instance, IBM 10 GbE RoCE Express will be used.

- RoCE Express2, which is a generic term representing an IBM RoCE Express2® feature that might operate in either 10 GbE or 25 GbE link speed. When this term is used in this information, the processing being described applies to either link speed. If processing is applicable to only one link speed, the full terminology, for instance, IBM 25 GbE RoCE Express2 will be used.
- RoCE Express3, which is a generic term representing an IBM RoCE Express3 feature that might operate in either 10 GbE or 25 GbE link speed. When this term is used in this information, the processing being described applies to either link speed. If processing is applicable to only one link speed, the full terminology, for instance, IBM 25 GbE RoCE Express3 will be used.
- RDMA network interface card (RNIC), which is used to refer to the IBM 10 GbE RoCE Express, IBM® 10 GbE RoCE Express2, IBM 25 GbE RoCE Express2, IBM 10 GbE RoCE Express3, or IBM 25 GbE RoCE Express3 feature.
- Shared RoCE environment, which means that the "RoCE Express" feature can be used concurrently, or shared, by multiple operating system instances. The feature is considered to operate in a shared RoCE environment even if you use it with a single operating system instance.

Clarification of notes

Information traditionally qualified as Notes is further qualified as follows:

Attention
Indicate the possibility of damage

Guideline
Customary way to perform a procedure

Note
Supplemental detail

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

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

Prerequisite and related information

z/OS Communications Server function is described in the z/OS Communications Server library. Descriptions of those documents are listed in “Bibliography” on page 203, in the back of this document.

Required information

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

Softcopy information

Softcopy publications are available in the following collection.

Titles	Description
IBM Z Redbooks	The IBM Z® subject areas range from e-business application development and enablement to hardware, networking, Linux®, solutions, security, parallel sysplex, and many others. For more information about the Redbooks® publications, see http://www.redbooks.ibm.com/ and http://www.ibm.com/systems/z/os/zos/zfavorites/.

Other documents

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

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

To find the complete z/OS library, visit the z/OS library in IBM Documentation (https://www.ibm.com/docs/en/zos).

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

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

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

Title	Number
z/OS UNIX System Services Planning	*GA32-0884*
z/OS UNIX System Services Programming: Assembler Callable Services Reference	*SA23-2281*
z/OS UNIX System Services User's Guide	*SA23-2279*
z/OS XL C/C++ Runtime Library Reference	*SC14-7314*
Open Systems Adapter-Express Customer's Guide and Reference	*SA22-7935*

Redbooks publications

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

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

Where to find related information on the Internet

z/OS

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

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

z/OS Internet Library

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

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

z/OS Communications Server product

The page contains z/OS Communications Server product introduction

https://www.ibm.com/products/zos-communications-server

IBM Communications Server product support

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

https://www.ibm.com/mysupport

IBM Communications Server performance information

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

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

IBM Systems Center publications

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

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

z/OS Support Community

Search the z/OS Support Community Library for Techdocs (including Flashes, presentations, Technotes, FAQs, white papers, Customer Support Plans, and Skills Transfer information)

z/OS Support Community

Tivoli® NetView® for z/OS

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

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

RFCs

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

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

Internet drafts

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

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

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

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

DNS websites

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

USENET news groups
comp.protocols.dns.bind

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

BIND Users

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

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

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

The z/OS Basic Skills Information Center

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

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

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

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

Summary of changes for New Function Summary

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

Changes made in z/OS Version 2 Release 5

This document contains information previously presented in z/OS Communications Server: New Function Summary, which supported z/OS Version 2 Release 4.

New information

The following information is new.

June 2023 refresh

- "z/OS UNIX syslogd support for secure logging over TCP" on page 42 with APAR PH47666
- "AT-TLS currency with System SSL with APAR PH49284" on page 44

October 2022 refresh

- "Communications Server exploitation of the IBM Function Registry for z/OS" on page 24 with SNA APAR OA63555

July 2022 refresh

- "AT-TLS support for x25519 and x448 key exchange for TLSv1.2" on page 46 with APAR PH45902

June 2022 refresh

- "OSA-Express Enhanced Inbound Blocking (EIB)" on page 26 with TCP/IP APAR PH44281 and SNA APAR OA62831
- "IBM zERT Network Analyzer passphrase and password management support" on page 49 with APAR PH43119

May 2022 refresh

- "Support for SMF compliance evidence" on page 47 with APAR PH37372

April 2022 refresh

"Communications Server support for RoCE Express3" on page 27 with APARs PH34117 and OA60855

March 2022 refresh

- "FTP server JES access control" on page 48 with APAR PH42618

December 2021 refresh

- "IBM Health Checker for the removal of VTAM LSA Architecture" on page 24 with APAR OA62208
- "IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity" on page 25 with APARs OA62208 and PH40875

Prior to December 2021 refresh

Chapter 3, "V2R5 new function summary," on page 23 includes descriptions for the new functions and enhancements introduced in this release and explains how to use them. Entries for the new functions and enhancements are added to Chapter 2, "Roadmap to functions," on page 19.

Changes made in z/OS Version 2 Release 4

This document contains information previously presented in z/OS Communications Server: New Function Summary, which supported z/OS Version 2 Release 3.

New

The following information is new.

May 2022 refresh

- "Support for SMF compliance evidence" on page 121 with APAR PH37372

March 2022 refresh

- "FTP server JES access control" on page 122 with APAR PH42618

January 2021 refresh

- "zERT Aggregation recording interval" on page 113

August 2020 refresh

- "Shared Memory Communications multiple IP subnet support (SMCv2)" on page 105

July 2020 refresh

- "IBM Health Checker for use of native TLS/SSL support for the FTP server" on page 125 with TCP/IP APAR PH24732 and SNA APAR OA59490

Prior to July 2020 refresh

- "IBM Health Checker for use of native TLS/SSL support for DCAS" on page 124 with TCP/IP APAR PH16144 and SNA APAR OA58255
- "IBM Health Checker for use of native TLS/SSL support for the FTP server" on page 125 with TCP/IP APAR PH21573 and SNA APAR OA59022
- "IBM Health Checker for use of native TLS/SSL support for the TN3270 server" on page 126 with TCP/IP APAR PH16144 and SNA APAR OA58255
- IBM zERT Network Analyzer database administration enhancements with APAR PH16223
- "Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions" on page 114 with VTAM APAR OA58300 and TCP/IP APAR PH16581
- Sysplex Autonomics for IPSec with APAR PH12788
- "SMTPD compatibility enhancements for CSSMTP" on page 140 with APAR PH18237

Chapter 5, "V2R4 new function summary," on page 99 includes descriptions for the new functions and enhancements introduced in this release and explains how to use them. Entries for the new functions and enhancements are added to Chapter 2, "Roadmap to functions," on page 19.

Changed information

The following information is changed.

Prior to 2020 refresh

- zERT Aggregation recording interval (APAR PH25049), see the following topics:
  - "z/OS Encryption Readiness Technology (zERT) aggregation" on page 134
  - "IBM zERT Network Analyzer" on page 137

Chapter 1. Planning to use new functions

These topics help you plan to use new functions:

Introduction to z/OS Communications Server

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

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

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

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

- The IBM Z product line consists of the IBM z13® (z13), IBM z13s® (z13s), IBM z14 (z14), IBM z15™ (z15), and IBM z16 (z16).
- The IBM zEnterprise® System (zEnterprise) product line consists of the IBM zEnterprise EC12 (zEC12), the IBM zEnterprise BC12 (zBC12), the IBM zEnterprise 196 (z196), and the IBM zEnterprise 114 (z114).
- The IBM System z10 product line includes IBM System z10 Enterprise Class (z10 EC) and the IBM System z10 Business Class (z10 BC).
- The IBM System z9® product line includes IBM System z9 Enterprise Class (z9® EC) (formerly known as the IBM System z9 109 [z9-109]), and the IBM System z9 Business Class (z9 BC).
- The IBM eServer™ zSeries product line includes the IBM eServer zSeries 990 (z990), and 890 (z890).
- The IBM System 390 (S/390®) product line includes the IBM S/390 Parallel Enterprise Server Generation 5 (G5) and Generation 6 (G6), and the IBM S/390 Multiprise 3000 Enterprise Server.

The z16, z15, z14, z13s,z13, zEC12, zBC12, z196, z114, z10 EC, z10 BC, z9 EC (formerly z9-109), z9 BC, z990, and z890 servers are also known as z/Architecture® servers. z/OS V2R5 Communications Server runs only in z/Architecture mode on IBM Z.

Determining which documents to use when upgrading

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

Table 1. Comparing documents used in migration	
Document name	**Descriptions**
z/OS Planning for Installation	This document helps you prepare to install z/OS by giving you information that you need to write an installation plan. To install means to perform the tasks necessary to make the system operational, starting with a decision to either install for the first time or upgrade, and ending when the system is ready for production. An installation plan is a record of the actions you need to take to install z/OS. **Recommendation:** It is recommended that you read this document. **Use this document as you prepare to install z/OS.**
Upgrading to z/OS V2R5	IBM no longer provides the *z/OS Migration* publication, GA32-0889, in a publication format. Since z/OS V2R2, the preferred method for learning about migration actions has been the z/OS Migration Workflow. Discovering, performing, and verifying many migration actions through the z/OSMF Workflows task instead of a more traditional book format allows for a tailored and specific upgrade path that is associated with a particular system. Beginning with z/OS V2R4,IBM provides migration tasks in a z/OSMF workflow, as well as a single exported file. By providing the migration materials in both formats, users still can enjoy the advantages of a z/OSMF workflow and be able to search, browse, and print in a more traditional format. It is strongly recommended that you plan for your next upgrade by having z/OSMF ready to use in at least one location in your enterprise. Notice that the exported format of the z/OS migration materials that can be read or printed for those without any z/OSMF capabilities will not be tailored for any environment. The z/OS Upgrade Workflow is provided in the git repository for IBM/IBM-Z-zOS, which already hosts the z/OS migration workflows for 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 Release Upgrade Reference Summary	This document describes the changes to interfaces for individual elements and features of z/OS. **Use this document as a reference to the new and changed commands, macros, panels, exit routines, data areas, messages, and other interfaces of individual elements and features of z/OS.**
z/OS Communications Server: New Function Summary	This document includes function summary topics to describe all the functional enhancements for the IP and SNA components of Communications Server, including task tables that identify the actions necessary to exploit new function. **Use this document as a reference to using all the enhancements of z/OS Communications Server.**

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

IP encryption features

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

The encryption features include these capabilities:

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

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

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

Planning checklist

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

Procedure

1. Understand your network topology, including the hardware and software in your network and your network configuration.
2. Understand that z/OS Communications Server is a base element of z/OS.

   Use the appropriate documents as you plan, upgrade, and install:

   - For information about migration and writing an installation plan, see "Determining which documents to use when upgrading" on page 1.
   - For information about installation, see these documents:
     - *z/OS Program Directory*
     - Preventative Service Planning (PSP) bucket (available by using IBMLINK)
     - *ServerPac: Installing Your Order*, if you use the ServerPac method to install z/OS
   - For information about storage requirements, see *z/OS Program Directory*, IBMLINK, or z/OS Communications Server Support. You can also see the storage estimate worksheets in z/OS Communications Server: SNA Network Implementation Guide.
3. Develop your education plan.
   a) Evaluate the z/OS V2R5 Communications Server features and enhancements by reading the new function summary topics in this document.
   b) Plan which new functions will be incorporated into your system.
4. Review and apply the Program Temporary Fixes (PTFs), including Recommended Service Upgrades (RSUs), for the current-minus-3 month plus all hipers and PEs. The PTFs are available monthly through the period for which the release is current and can be obtained by using IBMLINK. RSU integration testing for a release will be performed for five quarters after the general availability date for that release.
5. Get acquainted with the helpful information found at z/OS Communications Server Support.
6. In writing a test plan for z/OS, include test cases for these items:
   - TCP/IP applications
   - Key or critical SNA applications and Original Equipment Manufacturer (OEM) software products.

- User-written applications such as: Customer Information Control System (CICS®) sockets, Information Management System (IMS) sockets, REXX sockets, Sockets Extended, UNIX System Services sockets, and Macro Sockets
- Operator commands
- Your terminal and printer types

7. Back up your user exits and user modifications for later restore.
8. Install z/OS Communications Server with the other elements and features of z/OS. IBM has defined the appropriate product enablement settings in the IFAPRD00 member of SYS1.IBM.PARMLIB. For information about dynamic enablement, see z/OS Planning for Installation.
9. Complete post-installation activities:
   - Use z/OS Communications Server: IP Configuration Guide to customize your TCP/IP system.
   - Use the following information to customize your SNA system:
     - z/OS Communications Server: SNA Customization
     - z/OS Communications Server: SNA Network Implementation Guide
     - z/OS Communications Server: SNA Resource Definition Reference
   - Use z/OS Upgrade Workflow to determine migration actions.
   - Reinstall user exits.
   - Reinstall user modifications.
   - Update operating procedures and automation routines.
   - Activate new functions.
10. Complete functional and stress tests.

TCP/IP packaging process

As a result of the installation process for z/OS V2R5 Communications Server, the product is installed in both traditional MVS data sets and in files in the z/OS UNIX file system. For details on changes in the MVS data sets, see "MVS data sets" on page 4. For details on requirements for hierarchical file system files, see "File system files" on page 7.

MVS data sets

Table 2 on page 4 lists the distribution library data sets required by z/OS V2R5 Communications Server.

Table 2. Distribution library data sets

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

Table 2. Distribution library data sets (continued)	
Data set	**Description**
AEZAROE3	Reentrant object module for SEZAXMLB (z/OS UNIX support)
AEZARNT4	Reentrant object modules for RPC
AEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)
AEZASMP1	Sample source programs, catalog procedures, CLIST, and installation jobs
AEZAXLTD	Translated default tables
AEZAXLTK	Translated Kanji, Hangeul, and Traditional Chinese DBCS tables and codefiles
AEZAXLT1	Translation table SBCS source and DBCS source for Hangeul and Traditional Chinese
AEZAXLT2	TELNET client translation tables
AEZAXLT3	Kanji DBCS translation table source
ABLSCLI0	clists, execs, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSMSG0	messages, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSPNL0	panels, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables
ABLSTBL0	tables, IPCS clists, execs; IPCS messages; IPCS panels, IPCS tables

Table 3 on page 5 lists the target library data sets required by z/OS V2R5 Communications Server.

Table 3. Target library data sets	
Data set	**Description**
SEZACMAC	Client Pascal macros, C headers, and assembler macros
SEZACMTX	Load library for linking user modules and programs
SEZADBCX	Source for the Kanji, Hangeul, and Traditional Chinese DBCS translation tables
SEZADBRM	DBRM members
SEZADPIL	SNMP Distributed Programming Interface library
SEZADSIL	SNMP command processor and SNMPIUCV subtask for the NetView program, and the SQESERV module for the SNMP query engine
SEZADSIM	SNMP messages for the NetView program
SEZADSIP	SNMPIUCV initialization parameters for the NetView program
SEZAEXEC	CLISTs and REXX programs
SEZAINST	Installation samples and related members
SEZALIBN	NCS library system library
SEZALOAD	Executable load modules for concatenation to LINKLIB
SEZALNK2	LB@ADMIN for the NCS administrator
SEZALPA	Executable load modules for concatenation to LPALST
SEZAMENU	ISPF messages
SEZANCLS	NetView SNMP CLISTs

Table 3. Target library data sets (continued)	
Data set	**Description**
SEZANMAC	C headers and assembler macros for z/OS UNIX and TCP/IP Services APIs
SEZANPNL	NetView SNMP panels
SEZAOLDX	X Window System library (X10 compatibility routines)
SEZAPENU	ISPF panels
SEZARNT1	Reentrant object module for SEZAX11L, SEZAXTLB, SEZAOLDX, and SOCKETS
SEZARNT2	Reentrant object module for SEZAXAWL
SEZARNT3	Reentrant object module for SEZAXMLB
SEZARNT4	Reentrant object modules for RPC
SEZAROE1	Reentrant object module for SEZAX11L, SEZAXTLB, and SEZAOLDX (z/OS UNIX support)
SEZAROE2	Reentrant object module for SEZAXAWL (z/OS UNIX support)
SEZAROE3	Reentrant object module for SEZAXMLB (z/OS UNIX support)
SEZARPCL	Remote procedure call library
SEZATCP	Executable load modules for STEPLIB or LNKLST concatenation
SEZATCPX	Source for the country SBCS translation tables
SEZATELX	Source for the TELNET country translation tables
SEZAXAWL	Athena widget set
SEZAXLD1	Translated default tables
SEZAXLD2	Translated Kanji, Hangeul, and Traditional Chinese DBCS default tables and DBCS codefiles for TELNET transform mode
SEZAXMLB	Motif widget set
SEZAXTLB	X Window System Toolkit library
SEZAX11L	X Window System library

Table 4 on page 6 lists the shared distribution and target library data sets required by z/OS V2R5 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

Table 4. Shared distribution and target library data sets (continued)	
Data set	**Description**
SYS1.PARMLIB / SYS1.APARMLIB	IBM-supplied and installation-created members, which contain lists of system parameter values
SYS1.SAXREXEC	Contains system REXX programs
SYS1.SBLSCLI0	IPCS REXX execs and CLISTs
SYS1.SBLSKEL0	ISPF skeletons for the IPCS dialog
SYS1.SBLSMSG0	ISPF messages for the IPCS dialog
SYS1.SBLSPNL0	ISPF panels for the IPCS dialog
SYS1.SBLSTBL0	ISPF tables for the IPCS dialog

File system files

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

Defining SNA data sets

This section describes z/OS data sets that you need to define or modify for z/OS V2R5 Communications Server. Table 5 on page 7 shows the z/OS data sets that contain information for z/OS V2R5 Communications Server, and Table 6 on page 9 shows the z/OS data sets that contain information for VTAM.

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

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

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

Table 5. z/OS data sets containing information for z/OS Communications Server		
Name of data set	**Contents**	**Comments**
SYS1.DSDB1	Data files of APPN directory information	Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes. In a sysplex, this data set must be unique for each system; it may not be shared.
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. In a sysplex, this data set must be unique for each system; it may not be shared.

Table 5. z/OS data sets containing information for z/OS Communications Server (continued)		
Name of data set	**Contents**	**Comments**
SYS1.DSDBCTRL	Current status of SYS1.DSDB1 and SYS1.DSDB2	Required for APPN directory checkpointing function; must be allocated before z/OS Communications Server initialization. This data set cannot be allowed to span multiple volumes. In a sysplex, this data set must be unique for each system; it may not be shared.
SYS1.DUMPxx	Records of SVC DUMP	Required for diagnosis.
SYS1.LINKLIB	z/OS Communications Server initialization module, ISTINM01, which is used when z/OS Communications Server is started	Required.
	Logon manager load modules	Required for logon manager.
SYS1.LOGREC	z/OS Communications Server error records	Required.
SYS1.LPALIB	z/OS Communications Server load modules and user-written exit routines to be loaded into the shared link pack area	Required.
SYS1.MACLIB	z/OS Communications Server application program interface macros	Required.
SYS1.MIGLIB	z/OS Communications Server formatted dump routines for the interactive problem control system (IPCS) and the z/OS Communications Server VIT Analysis Tool module, ISTRAFT1, which is used for problem diagnosis	Required.
SYS1.NUCLEUS	z/OS Communications Server resident SVCs and abnormal termination modules	Required.
SYS1.PARMLIB	IBM-supplied and installation-created members, which contain lists of system parameter values	Required. This may also be a data set in the logical parmlib concatenation.
SYS1.PROCLIB	JCL for started tasks	Required for logon manager.
SYS1.SBLSCLI0	IPCS REXX execs and CLISTs	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information.
SYS1.SBLSKEL0	ISPF skeletons for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information.
SYS1.SBLSMSG0	ISPF messages for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information.

Table 5. z/OS data sets containing information for z/OS Communications Server (continued)		
Name of data set	**Contents**	**Comments**
SYS1.SBLSPNL0	ISPF panels for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information.
SYS1.SBLSTBL0	ISPF tables for the IPCS dialog	Required for z/OS Communications Server dump analysis enhancements and VIT analysis.
SYS1.SISTCLIB	z/OS Communications Server load modules to be loaded into common service area and extended common service area (CSA/ECSA) storage	Required.
SYS1.SISTDAT1	Online tools	Optional. Use this library only if you intend to use the online information tools included with z/OS Communications Server.
SYS1.SISTDAT2	Message skeleton file for translation	Required. See z/OS Communications Server: SNA Network Implementation Guide.
SYS1.SISTMAC1	z/OS Communications Server macros used to build user tables and parameter lists to build installation exits	Required.
SYS1.TRACE	GTF trace records	Required to run external trace. **Note:** For information about using multiple SYS1.TRACE data sets, see the z/OS MVS Diagnosis: Tools and Service Aids.
SYS1.TRSDB	Network topology database	Required for APPN topology database checkpointing function; must be allocated before initialization. This data set cannot be allowed to span multiple volumes. In a sysplex, this data set must be unique for each system; it may not be shared.
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. In a sysplex, these data sets must be unique for each system; it may not be shared.

Table 6 on page 9 shows the z/OS data sets that contain VTAM information.

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

Table 6. z/OS data sets containing information for VTAM (continued)		
Name of data set	**Contents**	**Comments**
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.VTAMLIB	• Load modules for z/OS Communications Server • User-defined tables, default tables, and exit routines	Only z/OS Communications Server load modules are required. Must be listed in an IEAAPFxx parmlib member.
SYS1.VTAMLST	z/OS Communications Server definition statements and start options	Required; created by user before starting z/OS Communications Server.
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. In a sysplex, these data sets must be unique for each system; it may not be shared.
SYS1.NODELST	z/OS Communications Server status of major nodes	Required if restart of all previously active major nodes is desired. In a sysplex, this data set must be unique for each system; it may not be shared.

Data sets containing information for z/OS V2R5 Communications Server

This section describes data sets that contain information for z/OS V2R5 Communications Server.

SYS1.SISTCLIB

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

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

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

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

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

SYS1.VTAMLST

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

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

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

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

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

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

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

   - COSAPPN

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

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

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

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

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

Guidelines:

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

without changing a corresponding NCP definition statement can cause serious errors that are difficult to diagnose.

SYS1.VTAMLIB

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

SYS1.VTAMLIB is used to store these user tables:

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

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

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

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

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

Parmlib member for communications storage manager (CSM)

Communications storage manager (CSM) supports storage above the 64-bit address bar.

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

The parameter member IVTPRM00 can be found in:

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

IVTPRM00 has this format:

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

       FIXED MAX(maxfixK|M)

       ECSA MAX(maxecsaK|M)

       HVCOMM MAX(maxhvcommM)

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

Rules:

- Each line in IVTPRM00 must start in column one.
- FIXED and MAX or ECSA and MAX keywords must be separated by one or more spaces. It must be completed with its values on the same line.

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

This describes the variable fields in the CSM parmlib member:

maxfix
A decimal integer specifying the maximum bytes of fixed storage to be dedicated for use by CSM. The range is from 1024 KB to 30720 MB. The default value is 512 MB.

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

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

maxhvcomm
A decimal integer specifying the maximum bytes of HVCOMM storage to be dedicated for use by CSM. The range is from 100 MB to 999999 MB. The default value is 2000 MB.

KB
Denotes size in kilobytes

MB
Denotes size in megabytes.

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

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

ECSA
Buffers are allocated from ECSA storage.

DSPACE
Buffers are allocated from data space storage.

HVCOMM
Buffers are allocated from high virtual common 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 for ECSA and data space pools

4 KB
1 - 256

16 KB
1 - 256

32 KB
1 - 128

60 KB
1 - 68

180 KB
1 - 22

Bufsize
Range for Expbuf for HVCOMM pools

4 KB
1 - 1024

16 KB
1 - 512

32 KB
1 - 256

60 KB
1 - 136

180 KB
1 - 45

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 on page 14 and Table 8 on page 14 show 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 for ECSA and data space

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

Table 8. IBM-supplied default values for CSM buffer pools for HVCOMM

Bufsize	**4 KB**	**16 KB**	**32 KB**	**60 KB**	**180 KB**
EXPBUF	256	64	32	17	5
INITBUF	256	64	32	17	5
MINFREE	32	8	4	4	2

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

IBM Health Checker for z/OS can be used to check whether appropriate values are defined for the maximum amount of storage to be dedicated to fixed buffers and ECSA buffers in CSM. For more details about IBM Health Checker for z/OS, see IBM Health Checker for z/OS: User's Guide.

Table 9. 64 bit enablement of CSM	
Task	**Reference**
Optionally update the IVTPRM00 parmlib member to specify the parameters to use when you allocate storage for CSM buffer use above the bar.	z/OS Communications Server: New Function Summary
Issue the **D CSM** command to monitor the use of storage above the bar that is managed by CSM.	z/OS Communications Server: SNA Operation
Issue the **MODIFY CSM** command to update values for storage above the bar that is managed by CSM.	z/OS Communications Server: SNA Operation

APPN checkpointing data sets

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

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

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

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

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

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

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

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

SYS1.TRSDB is required for checkpointing the network topology database. The information in this data set is used to initialize the network topology database whenever z/OS V2R5 Communications Server is restarted. The network topology database is written to this file whenever a `MODIFY CHKPT TYPE=TOPO` or `TYPE=ALL, HALT`, or `HALT QUICK` command is issued.

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

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

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

- Specify these DCB subparameters for SYS1.DSDBCTRL:

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

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

Guidelines:

- The DSDBCTRL is a fixed, 20-byte file; it requires a 20-byte block.

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

Using configuration restart data sets

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

Procedure

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

1. Use a DD statement to define a configuration restart VSAM data set for each major node. The *ddname* must match the *ddname* on the CONFGDS operand of either the PCCU definition statement for the associated NCP or the VBUILD definition statement for the associated major node. There are no z/OS Communications Server restrictions on this data set name.

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

   ```
   DEFINE
     CLUSTER(NAME(RESTART) -
             VOL(PUBLIC) -
             KEYS(18 0) -
             DATA(NAME(RESTART.DATA) -
             RECORDS(200 20) -
             RECORDSIZE(46 158)) -
     INDEX(NAME(RESTARTI.INDEX) -
             TRACKS(1))
   ```
2. Code the INDEX operand on the DEFINE command, or let it default. (See the sample DEFINE command.) The data set must be indexed.
3. Code KEYS (18 0). A key length of 18 bytes and an offset of 0 bytes are required.
4. Code RECORDSIZE (46 158). The average record size must be 46 bytes, and the maximum record size must be 158 bytes.
5. Make sure that the number of records in the file is equal to the number of minor nodes defined in the major node. When you choose the number of records for a switched major node, include each PATH definition statement. Therefore, the primary allocation should be the number of minor nodes in the major node, and the secondary allocation should be about 0.1 times the number of minor nodes.
6. When you change a major node definition in SYS1.VTAMLST, do not use the WARM start option when activating the new definition for the first time.

Dynamically configuring data sets for channel-attached devices

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

Procedure

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

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

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

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

   ```
   DEFINE
     CLUSTER(NAME('VSAM.AUTOCKPT') -
             VOL(PUBLIC) -
             KEYS(4 0) -
             DATA(NAME('VSAM.AUTOCKPT.DATA')-
             RECORDS(200 20) -
             RECORDSIZE(24 136)) -
     INDEX(NAME(VSAM.AUTOCKPT.INDEX) -
             TRACKS(1))
   ```
5. Add this data set using the AUTOCKPT DD statement in the z/OS Communications Server start procedure:

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

First Failure Support Technology

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

Defining a NODELST data set

You can define a NODELST data set to maintain a list of major nodes that are active at one time. If you use the NODELST facility, you need to define VSAM data sets.

Procedure

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

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

   ```
   DEFINE
     CLUSTER(NAME(NODLST1) -
             VOL(PUBLIC) -
   ```

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

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

Results

You can use defaults for all other data characteristics.

Chapter 2. Roadmap to functions

This topic includes a roadmap table to all of the functions and enhancements that were introduced in z/OS V2R5 Communications Server and z/OS V2R4 Communications Server.

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

Table 10. Roadmap to functions

Functional enhancement	Exploitation actions
Enhancements introduced in z/OS V2R5 Communications Server	
For all V2R5 new function APARs, see z/OS Communications Server V2R5 New Function APAR Summary.	
"z/OS UNIX syslogd support for secure logging over TCP" on page 42 with APAR PH47666	Yes
"AT-TLS currency with System SSL with APAR PH49284" on page 44	Yes
"Communications Server exploitation of the IBM Function Registry for z/OS" on page 24 with SNA APAR OA63555	Yes
"AT-TLS support for x25519 and x448 key exchange for TLSv1.2" on page 46 with APAR PH45902	Yes
"Support for SMF compliance evidence" on page 47 with APAR PH37372	Yes
"FTP server JES access control" on page 48 with APAR PH42618	Yes
"IBM zERT Network Analyzer passphrase and password management support" on page 49 with APAR PH43119	Yes
"IBM Health Checker for the removal of VTAM LSA Architecture" on page 24 with APAR OA62208	Yes
"IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity" on page 25 with APARs OA62208 and PH40875	Yes
"Ping output enhanced to provide microsecond precision" on page 38	No
"zERT policy-based enforcement" on page 51	Yes
"AT-TLS currency with System SSL" on page 50	Yes
"AT-TLS and IPsec certificate diagnostics" on page 56	Yes
"Notification of availability of TCP/IP extended services" on page 39	Yes
"IPsec certificate reporting enhancements" on page 57	No
"OSA-Express Enhanced Inbound Blocking (EIB)" on page 26 with TCP/IP APAR PH44281 and SNA APAR OA62831	Yes
"Communications Server support for RoCE Express3" on page 27 with TCP/IP APAR PH34117	Yes
"Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)" on page 30	Yes
"zERT Aggregation recording interval" on page 35	Yes
"Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions" on page 36	Yes

Table 10. Roadmap to functions (continued)

Functional enhancement	Exploitation actions
"Sysplex Autonomics for IPSec" on page 58	Yes
"IBM zERT Network Analyzer database administration enhancements" on page 60	Yes
"SMTPD compatibility enhancements for CSSMTP" on page 62	Yes
Enhancements introduced in z/OS V2R4 Communications Server	
For all V2R4 new function APARs, see z/OS Communications Server V2R4 New Function APAR Summary.	
"Communications Server exploitation of the IBM Function Registry for z/OS" on page 99 with SNA APAR OA63555	Yes
"Support for SMF compliance evidence" on page 121 with APAR PH37372	Yes
"FTP server JES access control" on page 122 with APAR PH42618	Yes
"IBM zERT Network Analyzer passphrase and password management support" on page 123 with APAR PH43119	Yes
"IBM Health Checker for the removal of VTAM LSA Architecture" on page 99 with APAR OA62208	Yes
"IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity" on page 100 with APARs OA62208 and PH40875	Yes
"OSA-Express Enhanced Inbound Blocking (EIB)" on page 101 with TCP/IP APAR PH44281 and SNA APAR OA62831	Yes
"Communications Server support for RoCE Express3" on page 103 with APARs PH34117 and OA60855	Yes
"Shared Memory Communications multiple IP subnet support (SMCv2)" on page 105 with TCP/IP APAR PH22695 and SNA APAR OA59152	Yes
"IBM Health Checker for use of native TLS/SSL support for DCAS" on page 124 with TCP/IP APAR PH16144 and SNA APAR OA58255	Yes
IBM Health Checker for use of native TLS/SSL support for the FTP server with TCP/IP APAR PH21573 and SNA APAR OA59022	Yes
"IBM Health Checker for use of native TLS/SSL support for the TN3270 server" on page 126 with TCP/IP APAR PH16144 and SNA APAR OA58255	Yes
Communications Server resolver enhancements	Yes
Sysplex Autonomics for IPSec with APAR PH12788, and Network Configuration Assistant APAR PH16303	Yes
IBM zERT Network Analyzer database administration enhancements with APAR PH24494	Yes
Communications Server QDIO display enhancements	Yes
"AT-TLS support for TLS v1.3" on page 131	Yes
"zERT Aggregation recording interval" on page 113 with APAR PH25049	Yes
"Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions" on page 114 with VTAM APAR OA58300 and TCP/IP APAR PH16581	Yes
"SMTPD compatibility enhancements for CSSMTP" on page 140 with APAR PH18237	Yes

Table 10. Roadmap to functions (continued)	
Functional enhancement	**Exploitation actions**
“Sysplex notification of TCP/IP stack join or leave” on page 116	Yes
“Network support for z/OS Container Extensions” on page 117	Yes
“Communications Server support for OSA-Express7S 25 GbE features” on page 107	Yes
“Communications Server support for 25 GbE RoCE Express2 features” on page 108	Yes
“HiperSockets Converged Interface support” on page 110	Yes
“IWQ support for IPSec” on page 119	Yes
“IBM zERT Network Analyzer” on page 137	Yes
“z/OS Encryption Readiness Technology (zERT) aggregation” on page 134	Yes
“TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication” on page 139	Yes
“Code page enhancements for CSSMTP” on page 142	Yes

Chapter 3. V2R5 new function summary

This information contains topics about every function or enhancement introduced in z/OS V2R5 Communications Server. The topics describe each function and present the following information, if applicable:

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

See Chapter 2, "Roadmap to functions," on page 19 for a complete list of the functional enhancements.

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

See z/OS Release Upgrade Reference Summary for information about new and changed messages and interfaces.

Support considerations in V2R5

z/OS V2R5 Communications Server rejects the invalid configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS for both the FTP client and the FTP server.

z/OS V2R5 Communications Server removes support for the following functions:

- Workload distribution to non-z/OS targets (IBM WebSphere® DataPower® appliances)
- Native TLS/SSL support from TN3270E Telnet server, FTP server, and DCAS
- Support for NCA policy import
- CMIP from VTAM
- Sysplex Distributor optimized load balancing with Cisco Multi-Node Load Balancer
- z/OS V2R5 Communications Server removes several migration health checks:
  - ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL
  - ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL
  - ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL
  - ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL
  - ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL
  - ZOSMIGV2R4_NEXT_CS_OSIMGMT

For more information about z/OS V2R5 Communications Server support considerations, see z/OS Upgrade Workflow.

Simplification

The following topics describe enhancements for simplification:

- "Communications Server exploitation of the IBM Function Registry for z/OS" on page 24
- "IBM Health Checker for the removal of VTAM LSA Architecture" on page 24
- "IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity" on page 25

Communications Server exploitation of the IBM Function Registry for z/OS

z/OS V2R5 Communications Server, with SNA APAR OA63555, is enhanced to register VTAM general information with the IBM Function Registry for z/OS. This information allows you to understand the extent of SNA application activity in your network.

Using Communications Server exploitation of the IBM Function Registry for z/OS

To use Communications Server exploitation of the IBM Function Registry for z/OS, complete the appropriate tasks in Table 11 on page 24.

Table 11. Task topics to enable Communications Server exploitation of the IBM Function Registry for z/OS

Task	Reference
Use the IBM FXEPRINT utility function Issue the DISPLAY FXE command	VTAM usage of IBM Function Registry for z/OS in z/OS Communications Server: SNA Network Implementation Guide

IBM Health Checker for the removal of VTAM LSA Architecture

z/OS V2R5 Communications Server, with SNA APAR OA62208, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies if VTAM Link Station Architecture (LSA) devices are in use. These devices are configured with MEDIUM=CSMACD in the XCA major node PORT statement.

Support for VTAM Link Station Architecture (LSA) devices will be withdrawn in future releases of IBM z/OS Communications Server.

Dependency:

To use the IBM Health Checker for the removal of VTAM LSA Architecture, perform the following steps:

- Apply the appropriate PTF for SNA APAR OA62208
- Start the IBM Health Checker for z/OS

Using the IBM Health Checker for the removal of VTAM LSA Architecture

To use the IBM Health Checker for the removal of VTAM LSA Architecture, perform the tasks in Table 12 on page 24.

Table 12. IBM Health Checker for the removal of VTAM LSA Architecture

Task/Procedure	Reference
To use this migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R5_NEXT_CS_LSA migration health check. 3. Review health check output messages ISTM051I or ISTM052E for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for the removal of VTAM LSA Architecture, see Table 13 on page 25.

Table 13. All related topics about IBM Health Checker for the removal of VTAM LSA Architecture	
Book name	**Topics**
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R5_NEXT_CS_LSA
z/OS Upgrade Workflow	*SNA and IP services: Prepare for the removal of support for LSA and LCS devices*
z/OS Communications Server: SNA Messages	• ISTM051I • ISTM052E

IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity

z/OS V2R5 Communications Server, with SNA APAR OA62208 and TCP/IP APAR PH40875, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies if TCP/IP profile statements DEVICE, LINK, and HOME for OSA-Express connectivity are in use.

Support for DEVICE/LINK/HOME TCP/IP profile statements for OSA-Express connectivity will be withdrawn in future releases of IBM z/OS Communications Server.

Dependency:

To use the IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity, perform the following steps:

- Apply the appropriate PTF for SNA APAR OA62208
- Apply the appropriate PTF for TCP/IP APAR PH40875
- Start the IBM Health Checker for z/OS

Using the IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity

To use the IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity, perform the tasks in Table 14 on page 25.

Table 14. IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity	
Task/Procedure	**Reference**
To use this migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R5_NEXT_CS_OSADLH migration health check. 3. Review health check output messages ISTM053I or ISTM054E for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity, see Table 15 on page 26.

Table 15. All related topics about IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity

Book name	Topics
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R5_NEXT_CS_OSADLH
z/OS Upgrade Workflow	*IP Services: Prepare for the removal of support for OSA DEVICE/LINK/HOME configuration*
z/OS Communications Server: SNA Messages	• ISTM053I • ISTM054E

Hardware support

The following topics describe enhancements for hardware support:

OSA-Express Enhanced Inbound Blocking (EIB)

In z/OS V2R5 Communications Server, with TCP/IP APAR PH44281 and SNA APAR OA62831, OSA-Express Enhanced Inbound Blocking (EIB) is a QDIO performance enhancement that might be beneficial for OSA interfaces with a high volume of inbound network bulk or streaming traffic.

Restriction:

QDIO Enhanced Inbound Blocking is supported on OSA-Express7s on z16 or later systems (with supporting MCL).

Using OSA-Express Enhanced Inbound Blocking (EIB)

To use OSA-Express Enhanced Inbound Blocking (EIB), perform the tasks in Table 16 on page 26.

Table 16. Task topics to enable OSA-Express Enhanced Inbound Blocking (EIB)

Task/Procedure	Reference
• Configure VTAM start option QDIOEIB to enable OSA-Express Enhanced Inbound Blocking. • Verify that the QDIOEIB start option is enabled.	• QDIOEIB start option in z/OS Communications Server: SNA Resource Definition Reference • DISPLAY VTAMOPTS command in z/OS Communications Server: SNA Operation
• Configure VTAM start option QDIOSTG with the following values: – MAX or 126 for 25 gigabit OSA features. – 126 for gigabit or 10 gigabit OSA features. • Verify that the QDIOSTG start option is enabled.	• QDIOSTG start option in z/OS Communications Server: SNA Resource Definition Reference • DISPLAY VTAMOPTS command in z/OS Communications Server: SNA Operation
• Verify that INBPERF DYNAMIC (with or without WORKLOADQ) is set on eligible OSA interfaces via Netstat DEvlinks.	• Interface statement in z/OS Communications Server: IP Configuration Reference

Table 16. Task topics to enable OSA-Express Enhanced Inbound Blocking (EIB) (continued)	
Task/Procedure	**Reference**
Display whether OSA-Express Enhanced Inbound Blocking is enabled by issuing the DISPLAY TCPIP,,OSAINFO command.	• DISPLAY TCPIP,,OSAINFO in z/OS Communications Server: IP System Administrator's Commands

To find all new and updated topics about OSA-Express Enhanced Inbound Blocking (EIB), see Table 17 on page 27.

Table 17. All related topics about OSA-Express Enhanced Inbound Blocking (EIB)	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Fixed storage considerations for OSA-Express interfaces in QDIO mode
z/OS Communications Server: IP Configuration Reference	• Interface statement • DEVICE and LINK - MPCIPA OSA-Express QDIO devices statement • INTERFACE-IPAQENET OSA-Express QDIO interfaces • INTERFACE-IPAQENET6 OSA-Express QDIO interfaces
z/OS Communications Server: IP System Administrator's Commands	• DISPLAY TCPIP,,OSAINFO • Netstat DEvlinks/-d report
z/OS Communications Server: SNA Operation	• DISPLAY VTAMOPTS command • MODIFY VTAMOPTS command • START command
z/OS Communications Server: SNA Resource Definition Reference	• QDIOEIB start option • Start options syntax diagrams • QDIOSTG start option
z/OS Communications Server: Quick Reference	• F VTAMOPTS command • Start options

Communications Server support for RoCE Express3

z/OS V2R5 Communications Server, with TCP/IP APAR PH34117, extends the Shared Memory Communications over Remote Direct Memory Access (SMC-R) function to support the next generation IBM RoCE Express3 feature. The IBM RoCE Express3 feature allows TCP/IP stacks on different LPARs within the same central processor complex (CPC) to leverage the power of these state-of-the-art adapters to optimize network connectivity for mission critical workloads by using Shared Memory Communications technology.

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

Dependencies: This function requires the IBM z16 or later systems. To enable the z/OS Communications Server support for RoCE Express3 features, complete the appropriate tasks in the following table.

Using Communications Server support for RoCE Express3

To use Communications Server support for RoCE Express3, complete the appropriate tasks in Table 18 on page 28.

Table 18. Task topics to enable Communications Server support for RoCE Express3

Task	Reference
Configure at least one IBM RoCE Express3 feature in HCD. For each RoCE Express3 port, configure the physical network ID (PNetID), the physical channel ID (PCHID), the Function ID (FID), the virtual function ID (VF), and the port number (PORTNUM).	z/OS HCD User's Guide
Configure or update the GLOBALCONFIG SMCR statement in the TCP/IP profile. • Use the FID values configured in HCD to define the PFID values that represent physically different RoCE Express3 features to provide full redundancy support. • Do not specify PortNum for RoCE Express3 PFIDs, or specify the PORTNUM value configured in HCD for the PFID.	• GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference • Shared Memory Communications over Remote Direct Memory Access in z/OS Communications Server: IP Configuration Guide
Optionally configure or update the PFID and SMCRIPADDR parameters on the SMCR configuration statement on one or more IPAQENET OSD interface statements to enable these interfaces for SMC-Rv2. Use the FID values configured in HCD to define PFID values that represent physically different RoCE Express3 features to provide full redundancy support.	• INTERFACE-IPAQENET OSA-Express QDIO interfaces in z/OS Communications Server: IP Configuration Reference • Shared Memory Communications multiple IP subnet support (SMCv2) in z/OS Communications Server: IP Configuration Guide
Display information about a RoCE Express3 interface by issuing the Netstat DEvlinks/-d command and specifying the name of the RoCE Express3 interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about Communications Server support for RoCE Express3, see Table 19 on page 29.

Table 19. All related topics about Communications Server support for RoCE Express3

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Shared Memory Communications multiple IP subnet support (SMCv2) • RoCE Express3 feature environment • Connectivity and gateway functions • Shared Memory Communications terms • VLANID considerations • Physical network considerations • System requirements for SMC-R in a shared RoCE environment • System requirements for SMC-D • Configuring Shared Memory Communications over RDMA • VTAM displays and tuning statistics
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement • INTERFACE-IPAQENET OSA-Express QDIO interfaces
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP/IP profile record Global configuration section • RDMA network interface card (RNIC) interface statistics record (subtype 44)
z/OS Communications Server: IP System Administrator's Commands	• Netstat CONFIG/-f report • Netstat DEvlinks/-d report
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command • MODIFY CSDUMP command
z/OS Communications Server: SNA Network Implementation Guide	• Resources automatically activated by VTAM
z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	• HCQ entry for invoking a RoCE HCQ operation (Part 1) • HCQ2 entry for invoking a RoCE HCQ operation (Part 2) • HCQ3 entry for invoking a RoCE HCQ operation (Part 3) • HCQ4 entry for invoking a RoCE HCQ operation (Part 4) • HCQ5 entry for invoking a RoCE HCQ operation (Part 5) • HCQ6 entry for invoking a RoCE HCQ operation (Part 6)
z/OS Communications Server: SNA Resource Definition Reference	• CSDUMP start option

Table 19. All related topics about Communications Server support for RoCE Express3 (continued)	
Book name	**Topics**
z/OS Communications Server: IP and SNA Codes	• Data link control (DLC) status codes
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ4336I
z/OS Communications Server: SNA Messages	• IST2361I • IST2396I • IST2444I
z/OS HCD User's Guide	N/A

Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

In z/OS V2R5 Communications Server, Shared Memory Communications - Direct Memory Access (SMC-D) is enhanced to remove the same IP subnet restriction by exploiting SMC-Dv2.
In z/OS V2R5 Communications Server, Shared Memory Communications - Remote Direct Memory Access (SMC-R) is enhanced to remove the same IP subnet restriction by exploiting SMC-Rv2.

In z/OS V2R5 Communications Server, SMC is enhanced to allow greater control of which peers are to perform SMC negotiation using SMC global filters.

Dependencies:

- SMC-Dv2 is enabled with new IBM Z capability provided by the IBM Z Internal Shared Memory (ISM) function. The new ISMv2 capability is available on IBM z15 or later systems. For IBM z15 T01, refer to the MCL number P46601.067 driver D41C. The ISMv2 support is in the base of the IBM z15 T02.
- SMC-Rv2 is supported on IBM z15 or later systems with the IBM RoCE Express2 10 GbE and 25 GbE features.

Restrictions:

SMC-Dv2 supports both IPv4 and IPv6. SMC-Rv2 supports IPv4 only.

Down-level SMC partners might require a toleration PTF. If you plan to enable SMCv2 on a host which has connections to a down-level SMC (SMC-Dv1 or SMC-Rv1) system (z/OS Communications Server, Linux on Z, and AIX®), the down-level host will require the following toleration maintenance applied prior to enabling SMC-Dv2:

- For z/OS Communications Server, the down-level host will need the appropriate PTF for PH17556.
- For Linux on Z, see the Linux on Z web page at https://linux-on-z.blogspot.com/p/smc-for-linux-on-ibm-z.html for information related to toleration requirements.
- For AIX, see the AIX web page at https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/rdma/smc_r.html for information related to toleration requirements.

Note: Failure to apply the proper toleration maintenance might result in connection hangs or failures when SMCv2 is enabled on z/OS.

Using the Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

To use the Shared Memory Communications multiple IP subnet support (SMCv2), perform the tasks in Table 20 on page 31 for SMC-Rv2.

Table 20. Shared Memory Communications multiple IP subnet support (SMC-Rv2)	
Task/Procedure	**Reference**
Determine if using SMC will be a benefit in this configuration by using SMCAT.	VARY TCPIP,,SMCAT about SMC Applicability Tool (SMCAT) in z/OS Communications Server: IP System Administrator's Commands
Understand the base principles of the SMC environment.	Shared Memory Communications in z/OS Communications Server: IP Configuration Guide
Understand the base SMC-R setup requirements.	Setting up the environment for Shared Memory Communications over RDMA in z/OS Communications Server: IP Configuration Guide
Configure SMCEID on the SMCGLOBAL parameter of the GLOBALCONFIG statement to enable z/OS CS exploitation of SMCv2.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Configure at least one RoCE Express2 feature in HCD. For each IBM RoCE Express2 port, configure the physical network identifier (PNetID), the physical channel identifier (PCHID), the function identifier (FID), the virtual function identifier (VF), and the port number (PORTNUM).	z/OS HCD User's Guide
Configure PFID, SMCRIPADDR and optionally SMCRMTU parameters on the SMCR configuration statement on one or more IPAQENET OSD interface statements to enable SMC-Rv2.	INTERFACE - IPAQENET OSA-Express QDIO interfaces statement in z/OS Communications Server: IP Configuration Reference
Optionally configure SMCPERMIT on the GLOBALCONFIG statement to specify which partners can participate in SMC.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Optionally configure SMCEXCLUDE on the GLOBALCONFIG statement to specify which partners will be not allowed to participate in SMC.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display whether SMCEID values were specified on SMCGLOBAL by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display whether SMCPERMIT values were specified on SMCGLOBAL by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display whether SMCEXCLUDE values were specified on SMCGLOBAL by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display SMC version used for a connection or link.	z/OS Communications Server: IP System Administrator's Commands: • Netstat ALL/-A report • Netstat DEvlinks/-d SMC report
Display all interfaces z/OS CS used for SMC communications.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display the RoCEv2 capable RNIC that is associated with an OSD interface by issuing the Netstat DEvlinks/-d command and specifying the OSD interface name.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

Table 20. Shared Memory Communications multiple IP subnet support (SMC-Rv2) (continued)	
Task/Procedure	**Reference**
Display SMCv2 Link Group information to verify your link groups are fully redundant to your SMC partners for high availability.	Netstat DEvlinks/-d SMC report in z/OS Communications Server: IP System Administrator's Commands
Display information about the dynamic RoCE TRLEs by issuing the D NET,ID=*trle*, or D NET,TRL,TRLE=*trle* command.	z/OS Communications Server: SNA Operation • DISPLAY ID command • DISPLAY TRL command
Display routing information to your SMC-Rv2 partners to verify you have redundant routes using SMC-Rv2 enabled OSA-Express interfaces.	Netstat ROUTe/-r report in z/OS Communications Server: IP System Administrator's Commands

To use the Shared Memory Communications multiple IP subnet support (SMCv2), perform the tasks in Table 21 on page 32 for SMC-Dv2.

Table 21. Shared Memory Communications multiple IP subnet support (SMC-Dv2)	
Task/Procedure	**Reference**
Determine if using SMC will be a benefit in this configuration by using SMCAT.	VARY TCPIP,,SMCAT about SMC Applicability Tool (SMCAT) in z/OS Communications Server: IP System Administrator's Commands
Understand the base principles of the SMC environment.	Shared Memory Communications in z/OS Communications Server: IP Configuration Guide
Understand the base SMC-D setup requirements.	Setting up the environment for Shared Memory Communications - Direct Memory Access in z/OS Communications Server: IP Configuration Guide
Configure SMCEID on the SMCGLOBAL parameter of the GLOBALCONFIG statement to enable z/OS CS exploitation of SMCv2.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Configure SYSTEMEID on the SMCD parameter of the GLOBALCONFIG statement to enable z/OS CS exploitation of SMC-Dv2.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Optionally configure SMCPERMIT on the GLOBALCONFIG statement to specify which partners can participate in SMC.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Optionally configure SMCEXCLUDE on the GLOBALCONFIG statement to specify which partners will be not allowed to participate in SMC.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display whether SMCEID values were specified on SMCGLOBAL by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display whether SMCPERMIT values were specified on SMCGLOBAL by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display whether SMCEXCLUDE values were specified on SMCGLOBAL by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands

Table 21. Shared Memory Communications multiple IP subnet support (SMC-Dv2) (continued)	
Task/Procedure	**Reference**
Display SMC version used for a connection or link.	z/OS Communications Server: IP System Administrator's Commands: • Netstat ALL/-A report • Netstat DEvlinks/-d SMC report
Display all interfaces z/OS CS used for SMC communications.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display information about the dynamic ISM TRLEs by issuing the D NET,ID=*trle*, or D NET,TRL,TRLE=*trle* command, which might now show **NA** for the PNETID.	z/OS Communications Server: SNA Operation • DISPLAY ID command • DISPLAY TRL command

To find all new and updated topics about Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2), see Table 22 on page 33.

Table 22. All related topics about Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Shared Memory Communications • Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2) • Setting up the environment for Shared Memory Communications over RDMA • Setting up the environment for Shared Memory Communications - Direct Memory Access • Physical network considerations • VLANID considerations • Configuring Shared Memory Communications - Direct Memory Access
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement • INTERFACE - IPAQENET OSA-Express QDIO interfaces statement

Table 22. All related topics about Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2) (continued)

Book name	Topics
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP connection termination record (subtype 2) • TCP/IP profile event record (subtype 4) – TCP/IP profile record Global configuration section – TCP/IP profile record interface section – TCP/IP profile record self-defining section – TCP/IP profile record Permit table for SMC Filter section – TCP/IP profile record Exclude table for SMC Filter section • SMC-D link statistics record (subtype 38) • SMC-D link state start record (subtype 39) • SMC-D link state end record (subtype 40) • SMC-R link group statistics record (subtype 41) • SMC-R link state start record (subtype 42) • SMC-R link state end record (subtype 43) • RDMA network interface card (RNIC) interface statistics record (subtype 44)
z/OS Communications Server: IP Diagnosis Guide	• Diagnosing problems with Shared Memory Communications • Physical network ID configuration issues • No associated subnet mask
z/OS Communications Server: IP System Administrator's Commands	• DISPLAY TCPIP,,NETSTAT • VARY TCPIP,,SMCAT • Netstat ALL/-A report • Netstat CONFIG/-f report • Netstat DEvlinks/-d report
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command
z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	• ENFx entry for ENF exit • RPLA entry for invoking a RoCE Poll command (Part 3)
z/OS Communications Server: SNA Network Implementation Guide	Resources automatically activated by VTAM
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD1978I • EZD2051I • EZD2056I • EZD2057I

Table 22. All related topics about Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2) (continued)	
Book name	**Topics**
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ0841I • EZZ0842I • EZZ0843I • EZZ0844I • EZZ0845I • EZZ0846I • EZZ0847I • EZZ0848I
z/OS Communications Server: SNA Messages	• IST2396I • IST2398I • IST2406I • IST2418I • IST2421I • IST2464I • IST2465I • IST2466I • IST2467I

Scalability and performance

The following topics describe enhancements for scalability and performance:

- "zERT Aggregation recording interval" on page 35
- "Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions" on page 36

zERT Aggregation recording interval

z/OS V2R5 Communications Server provides a zERT Aggregation recording interval that is not bound to the system SMF interval. This interval allows zERT summary records to be generated at an interval that can range from 1 to 24 hours.

zERT summary records can be collected as SMF type 119, subtype 12 records in the System Management Facility data sets or log streams. zERT summary records can also be collected by a real-time NMI application using the SYSTCPES service.

Warning:

Decreasing the frequency at which zERT summary records are written can increase the amount of 64-bit pageable, private memory needed. This is because zERT aggregation information is held longer in memory before being captured in SMF records.

Using the zERT Aggregation recording interval

To use the zERT Aggregation recording interval, perform the tasks in Table 23 on page 36.

Table 23. zERT Aggregation recording interval	
Task/Procedure	**Reference**
Determine if you want to use the zERT aggregation recording interval.	Enabling a longer zERT aggregation recording interval in z/OS Communications Server: IP Configuration Guide
Enable the zERT aggregation recording interval using the new INTVAL and SYNCVAL sub-parameters on the GLOBALCONFIG ZERT AGGREGATION statement.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display zERT aggregation recording interval settings.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands

To find all new and updated topics about zERT Aggregation recording interval, see Table 24 on page 36.

Table 24. All related topics about zERT Aggregation recording interval	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Enabling a longer zERT aggregation recording interval • z/OS Encryption Readiness Technology (zERT) Concepts • How does zERT aggregation provide the information? • Enabling zERT aggregation • Setting up TCP/IP operating characteristics in PROFILE.TCPIP
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement
z/OS Communications Server: IP System Administrator's Commands	• D TCPIP,,STOR command • Netstat CONFIG/-f report
z/OS Communications Server: IP Programmer's Guide and Reference	• Format and details for poll-type requests • TCP/IP statistics record (subtype 5) • zERT Summary record (subtype 12) • TCP/IP profile record Global configuration section
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ8455I

Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions

z/OS V2R5 Communications Server is enhanced to support inbound workload queueing for IBM z/OS Container Extensions (zCX) workloads for OSA-Express in QDIO mode.

Inbound workload queueing uses multiple input queues for each QDIO data device (subchannel device) to improve TCP/IP stack scalability and general network optimization. To implement the performance improvements for zCX workloads, enable inbound workload queueing to process zCX, IPSec, EE, sysplex distributor, and streaming bulk data traffic all concurrently with other types of inbound QDIO traffic. When you enable these improvements for a QDIO interface, zCX, inbound IPSec, EE, sysplex distributor, and

streaming bulk data traffic are each processed on their own ancillary input queue (AIQ). All other inbound traffic is processed on the primary input queue.

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

Dependencies:

- This function is limited to OSA-Express6S Ethernet features or later in QDIO mode running on IBM z14® or later systems. For more information about the QDIO inbound workload queueing function and the OSA-Express features that support it, see QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide. See the 3906DEVICE or 3907DEVICE Preventive Service Planning (PSP) bucket for more information.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

Using Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions

To enable IWQ support for z/OS Container Extensions, complete the appropriate tasks in Table 25 on page 37.

Table 25. Task topics to enable IWQ support for z/OS Container Extensions

Task	Reference
Enable inbound workload queueing for a specific QDIO interface by specifying the WORKLOADQ parameter on the IPAQENET or IPAQENET6 INTERFACE statement (if not already configured).	• See the following statements in z/OS Communications Server: IP Configuration Reference: – INTERFACE-IPAQENET OSA-Express QDIO interfaces – INTERFACE-IPAQENET6 OSA-Express QDIO interfaces • Steps for enabling QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide
Display whether inbound workload queueing is in effect for the QDIO interface by issuing the **`Netstat DEvlinks/-d`** command.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display whether inbound workload queueing is in effect for the QDIO interface and display the workload queueing functions and queue IDs for that interface by issuing the **`DISPLAY NET,ID=trle`** command or the **`DISPLAY NET,TRL,TRLE=trle`** command.	See the following topics in z/OS Communications Server: SNA Operation: • DISPLAY ID command • DISPLAY TRL command
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by initiating VTAM tuning statistics for the QDIO interface.	MODIFY TNSTAT command in z/OS Communications Server: SNA Operation
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by using the TCP/IP callable NMI GetIfStatsExtended request.	TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer's Guide and Reference
Determine the QID on which a specific packet was received, and the associated workload queueing function, from a packet trace.	Formatting packet traces using IPCS in z/OS Communications Server: IP Diagnosis Guide

Table 25. Task topics to enable IWQ support for z/OS Container Extensions (continued)	
Task	**Reference**
Determine the QID on which a specific packet was received from an OSAENTA trace.	Formatting OSA traces using IPCS in z/OS Communications Server: IP Diagnosis Guide

To find all related topics about IWQ support for z/OS Container Extensions, see Table 26 on page 38.

Table 26. All related topics about IWQ support for z/OS Container Extensions	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• QDIO inbound workload queueing
z/OS Communications Server: IP Configuration Reference	• INTERFACE-IPAQENET OSA-Express QDIO interfaces • INTERFACE-IPAQENET6 OSA-Express QDIO interfaces
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP/IP callable NMI (EZBNMIFR)
z/OS Communications Server: IP Diagnosis Guide	• Formatting packet traces using IPCS • Formatting OSA traces using IPCS
z/OS Communications Server: IP System Administrator's Commands	• DISPLAY TCPIP,,OSAINFO • Netstat DEvlinks/-d report
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command • MODIFY TNSTAT command
z/OS Communications Server: SNA Messages	• IST1221I • IST1230I • IST1233I

Systems management

The following topic describes enhancements for systems management:

Ping output enhanced to provide microsecond precision

z/OS V2R5 Communications Server enhances the output for the TSO PING command and the z/OS UNIX ping command to provide the response time with a precision of microseconds.

Using the Ping output enhanced to provide microsecond precision

To use the Ping output enhanced to provide microsecond precision, perform the tasks in Table 27 on page 39.

Table 27. Ping output enhanced to provide microsecond precision	
Task/Procedure	**Reference**
Issue the TSO PING command or the z/OS UNIX ping command.	Ping in z/OS Communications Server: IP System Administrator's Commands

To find all new and updated topics about Ping output enhanced to provide microsecond precision, see Table 28 on page 39.

Table 28. All related topics about Ping output enhanced to provide microsecond precision	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Verifying connections with Netstat, Ping, and Traceroute • Activating the quick start Security Association
z/OS Communications Server: IP System Administrator's Commands	• MVS console invocation of the EZACMD command • NetView invocation of the EZACMD command • The TSO PING command: Send an echo request • The z/OS UNIX ping command: Send an echo request

Notification of availability of TCP/IP extended services

z/OS V2R5 Communications Server has enhanced TCP/IP to dynamically generate a new console message (EZD1314I), Event Notification Facility signal, and Name/Token pair when the TCP/IP stack and all its extended stack services are fully initialized. You can use TCP/IP profile configuration to determine which extended services are required based on your needs.

Using the notification of availability of TCP/IP extended services

To use the notification of availability of TCP/IP extended services, perform the tasks in Table 29 on page 39.

Table 29. Notification of availability of TCP/IP extended services	
Task/Procedure	**Reference**
Configure one of the options on the new GLOBALCONFIG POLICYREQUIRED parameter or take the default option.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Configure one of the options on the new GLOBALCONFIG IKEDREQUIRED parameter or take the default option.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference

Table 29. Notification of availability of TCP/IP extended services (continued)	
Task/Procedure	**Reference**
To programmatically determine if the TCP/IP stack and its extended services are initialized, create an ENF exit to listen for the ENF80 signal with the corresponding qualifier.	• z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG: – ENFREQ — Listen for system events – Table: ENF macro event codes • z/OS Communications Server: IP Programmer's Guide and Reference: – EZAENF80 Parameter list for ENF event code 80 listen exits – Using ENF event code 80 to notify applications of complete initialization of the TCP/IP stack and extended services
Another step you should perform to programmatically determine if the TCP/IP stack and its extended services are initialized is to retrieve the name/token pair. A name/token pair will be created at the same time the ENF signal is issued and is used to close a timing window that exists where an ENF signal can be missed if the signal is issued before the listener is started. The user_name value of the name/token pair is composed of the constant EZBSTKUP followed by the stack jobname padded with blanks (x'40'). An example of this is 'EZBSTKUPTCPCS1 '. An additional name/token pair will be generated when running in an INET environment where the stack jobname portion of the user_name will be the constant INET padded with 4 bytes of blanks (x'40404040'). An example of this is 'EZBSTKUPINET '.	• z/OS MVS Programming: Assembler Services Reference IAR-XCT: – IEAN4RT - Retrieve the token from a name/token pair (64-bit mode) – IEANTRT - Retrieve the token from a name/token pair (31-bit mode) • z/OS MVS Programming: Assembler Services Guide: – Understanding name/token pairs and levels • z/OS Communications Server: IP Programmer's Guide and Reference: – Using ENF event code 80 to notify applications of complete initialization of the TCP/IP stack and extended services
After starting the ENF listener and Name/Token Pair retrieval, if the receipt of the Name/Token Pair fails (meaning stack not ready yet) then wait for the ENF listen to pop, otherwise if the Name/Token receipt is successful (stack is ready) then cancel the ENF listen.	• z/OS MVS Programming: Assembler Services Reference IAR-XCT: – IEAN4RT - Retrieve the token from a name/token pair (IPV4) • z/OS Communications Server: IP Programmer's Guide and Reference: – Using ENF event code 80 to notify applications of complete initialization of the TCP/IP stack and extended services

To find all new and updated topics about notification of availability of TCP/IP extended services, see Table 30 on page 40.

Table 30. All related topics about notification of availability of TCP/IP extended services	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Verifying your configuration

Table 30. All related topics about notification of availability of TCP/IP extended services (continued)	
Book name	**Topics**
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP/IP profile record Global configuration section • EZAENF80 Parameter list for ENF event code 80 listen exits • Using ENF event code 80 to notify applications of complete initialization of the TCP/IP stack and extended services
z/OS Communications Server: IP Diagnosis Guide	• Diagnosing TCP/IP stack initialization problems
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZB6473I • EZD1176I • EZD1314I
z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG	• ENFREQ — Listen for system events • Table: ENF macro event codes
z/OS MVS Programming: Assembler Services Reference IAR-XCT	• IEAN4RT - Retrieve the token from a name/token pair (64-bit mode) • IEANTRT - Retrieve the token from a name/token pair (31-bit mode)
z/OS MVS Programming: Assembler Services Guide	• Understanding name/token pairs and levels

Enhancing security

The following topics describe enhancements for security:

z/OS UNIX syslogd support for secure logging over TCP

z/OS V2R5 Communications Server with APAR PH47666 provides syslog daemon support to receive and send messages over the network using TCP. These TCP connections can be protected with AT-TLS.

Restriction: The syslog daemon supports receiving and sending messages with octet-counted framing over TCP connections. The syslog daemon does not support receiving or sending messages with traditional (non-transparent) framing over TCP connections.

Dependencies: Syslogd is an AT-TLS aware application. To secure messages received by syslogd over a TCP connection, an AT-TLS server rule must be configured for the connection. To secure messages sent by syslogd over a TCP connection, an AT-TLS client rule must be configured for the connection.

Using z/OS UNIX syslogd support for secure logging over TCP

To use z/OS UNIX syslogd support for secure logging over TCP, complete the appropriate tasks in Table 31 on page 42.

Table 31. Task topics to enable z/OS UNIX syslogd support for secure logging over TCP

Task	Reference
Enable syslogd to receive messages from a remote syslogd over TCP in the clear • Use the syslogd -T start option • Define the TCP port to be used to receive messages in the /etc/services file • Reserve the TCP port to be used to receive messages with the PORT statement in the TCP/IP profile.	• *Processing message from remote system* section in Starting and stopping syslogd in z/OS Communications Server: IP Configuration Guide • *Syslogd start option syntax* section in Starting and stopping syslogd in z/OS Communications Server: IP Configuration Guide • Configuring syslogd to receive remote messages in z/OS Communications Server: IP Configuration Guide
Enable syslogd to receive messages from a remote syslogd over TCP protected by TLS • Use the syslogd -S start option • Define the TCP port to be used to receive secure messages in the /etc/services file • Reserve the TCP port to be used to receive secure messages with the PORT statement in the TCP/IP profile. • Create an AT-TLS server rule to protect the syslogd port	• *Processing message from remote system* section in Starting and stopping syslogd in z/OS Communications Server: IP Configuration Guide • *Syslogd start option syntax* section in Starting and stopping syslogd in z/OS Communications Server: IP Configuration Guide • Configuring syslogd to receive remote messages in z/OS Communications Server: IP Configuration Guide
If the -T or -S option is used to start syslogd and you also want to be able to receive messages from a remote syslogd over UDP, use the syslogd -U start option.	*Setup steps for the syslogd server to receive remote messages as UDP datagrams* in Considerations when receiving messages using UDP in z/OS Communications Server: IP Configuration Guide
Enable syslogd to send messages over TCP to a remote syslogd in the clear • Consider what priority of messages should be sent over the network • Create a rule in the syslogd configuration file (/etc/syslog.conf by default) using the -A(..) forwarding action to specify the destination.	• Configuring the z/OS syslogd to send messages to a remote syslogd in z/OS Communications Server: IP Configuration Guide • Remote destinations for syslogd in z/OS Communications Server: IP Configuration Reference

Table 31. Task topics to enable z/OS UNIX syslogd support for secure logging over TCP (continued)

Task	Reference
Enable syslogd to send messages over TCP to a remote syslogd protected by TLS • Consider what priority of messages should be sent over the network • Create a rule in the syslogd configuration file (/etc/syslog.conf by default) using the -A(...) forwarding action with secure="yes". • Create an AT-TLS client rule to protect messages sent to the remote syslogd	• Configuring the z/OS syslogd to send messages to a remote syslogd in z/OS Communications Server: IP Configuration Guide • Remote destinations for syslogd in z/OS Communications Server: IP Configuration Reference • AT-TLS policy statements in z/OS Communications Server: IP Configuration Reference
Consider using an IP filtering policy to limit which clients can connect to a syslogd TCP server. This applies to both a syslogd TCP server receiving messages in the clear and a syslogd TCP server receiving messages protected by TLS.	IPSec policy statements in z/OS Communications Server: IP Configuration Reference
Consider whether two instances of syslogd should be started – one to process messages generated by local applications and one to process messages received over the network. This can provide better performance in some environments.	• *Modes for running syslogd* in Starting and stopping syslogd in z/OS Communications Server: IP Configuration Guide • *Improving the efficiency of syslogd remote logging functions* section in Configuring syslogd to receive remote messages in z/OS Communications Server: IP Configuration Guide

To find all related topics about z/OS UNIX syslogd support for secure logging over TCP, see Table 32 on page 43.

Table 32. All related topics about z/OS UNIX syslogd support for secure logging over TCP

Book name	Topics
z/OS Communications Server: IP Configuration Reference	• PORT statement • Starting syslogd with a cataloged procedure • Starting syslogd from the UNIX shell • Syslogd environment variables • Parameters • Usage notes for syslogd • Supported destinations for syslogd • File destinations for syslogd • Remote destinations for syslogd

Table 32. All related topics about z/OS UNIX syslogd support for secure logging over TCP (continued)

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Environment variables • Logging of system messages • Other user IDs requiring z/OS UNIX superuser authority • Syslogd isolation • Configuring the syslog daemon • Starting and stopping syslogd • Configuring syslogd to receive remote messages • Usage notes • Considerations when receiving messages using UDP • Considerations when receiving messages using TCP • Configuring the z/OS syslogd to send messages to a remote syslogd • Interactions between syslogd and other components during IPL
z/OS UNIX System Services Messages and Codes	• FSUM1202 - FSUM 1204 • FSUM1206 • FSUM1211 • FSUM1222 • FSUM1226 • FSUM1228 • FSUM1229 • FSUM1239 • FSUM1276 - FSUM 1302

AT-TLS currency with System SSL with APAR PH49284

z/OS V2R5 Communications Server with APAR PH49284 enhances AT-TLS support.

z/OS V2R5 Communications Server with APAR PH49284 provides AT-TLS support for the following functions:

- TLS Version 1.3 sysplex session ticket support
- Domain-based server certificate validation during an SSL/TLS session negotiation

With APAR PH53064, you can configure these functions in IBM Network Configuration Assistant for z/OS Communications Server.

Dependencies:

- To use TLS Version 1.3 sysplex session tickets:
  - z/OS V2R5 System SSL APAR OA63252 is required.
  - GSKSRVR must be started for all systems in the sysplex acting as AT-TLS servers for the workload.
- To use domain-based server certificate validation, z/OS V2R5 System SSL APAR OA63164 is required.

Result:

In V2R5, TLSv1.3 performance improves significantly over V2R4 due to optimizations in cryptographic software and hardware acceleration of the RSASSA-PSS signature algorithm if you are using CryptoExpress adapters. However, you should still be aware that the CPU consumption of the TCP/IP address space will increase when you enable TLSv1.3. While TLSv1.3 provides stronger cryptographic protection for your TCP connections, it inherently uses more cryptographic operations and therefore consumes more CPU than TLSv1.2 when using comparable cipher suites and key exchange algorithms.

The magnitude of the CPU increase depends on a variety of factors, including the cipher suites you were using under TLSv1.2 (or earlier) and the level of hardware you are using (in the z15 and later models, CPACF acceleration of ECC operations can benefit TLSv1.3 performance).

Using AT-TLS currency with System SSL

To use AT-TLS currency with System SSL, complete the appropriate tasks in Table 33 on page 45.

Table 33. Task topics to enable AT-TLS currency with System SSL

Task	Reference
Understand the benefits and setup required for sysplex TLS Version 1.3 session ticket caching	• Session caching in z/OS Communications Server: IP Configuration Guide • Session ID (SID) and session ticket cache in z/OS Cryptographic Services System SSL Programming • SSL started task in z/OS Cryptographic Services System SSL Programming
Enable sysplex-wide TLSv1.3 session ticket caching for an AT-TLS server with the GSK_SYSPLEX_SESSION_TICKET_CACHE parameter on the TTLSGskAdvancedParms statement.	• Online help of IBM Network Configuration Assistant for z/OS Communications Server • GSK_SYSPLEX_SESSION_TICKET parameter on the TTLSGskAdvancedParms statement in z/OS Communications Server: IP Configuration Reference
Understand the benefits of domain-based server certificate validation as defined by RFC 6125	*Enabling an AT-TLS client to verify the server identity during the TLS handshake* section in Validating a host name against a certificate in z/OS Communications Server: IP Configuration Guide
Enable domain-based server certificate validation by providing one or more fully qualified DNS domain names on the AT-TLS client rule to use for verification • For a server certificate that includes a Subject Alternative Name (SAN) extension with a DNS domain name, provide references using the HostReferenceIdDNS parameter • For a server certificate with DNS domain name specified in the DN common name (and that does not include a SAN extension with a DNS domain name), provide references using the HostReferenceIdCN parameter • Values can be specified for both reference lists • If the server certificate can contain a wildcarded DNS domain name, enable wildcard support with the HostRefWildcardValidation parameter.	• Online help of IBM Network Configuration Assistant for z/OS Communications Server • HostReferenceIdDNS, HostReferenceIdCN, and HostRefWildcardValiation parameters on the TTLSEnvironmentAdvancedParms statement and TTLSConnectionAdvancedParms statement in z/OS Communications Server: IP Configuration Reference

Table 33. Task topics to enable AT-TLS currency with System SSL (continued)	
Task	**Reference**
Display AT-TLS policy using the z/OS UNIX pasearch command to query information from the Policy Agent.	The z/OS UNIX pasearch command: Display policies in z/OS Communications Server: IP System Administrator's Commands
Display AT-TLS policy for an active connection using the Netstat TTLS/-x command.	Netstat TTLS/-x report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about AT-TLS currency with System SSL, see Table 34 on page 46.

Table 34. All related topics about AT-TLS currency with System SSL	
Book name	**Topics**
z/OS Communications Server: IP Configuration Reference	• TTLSGskAdvancedParms statement • TTLSEnvironmentAdvancedParms statement • TTLSConnectionAdvancedParms statement • General syntax rules for Policy Agent
z/OS Communications Server: IP Configuration Guide	• Validating a host name against a certificate • Session caching
z/OS Communications Server: IP System Administrator's Commands	• COnn report examples • Report field descriptions • The z/OS UNIX pasearch command: Display policies

AT-TLS support for x25519 and x448 key exchange for TLSv1.2

z/OS V2R5 Communications Server with APAR PH45902 provides AT-TLS support for a TLSv1.2 server to specify which elliptic curves can be used for the handshake key exchange when an ephemeral ECDH (Elliptic curve Diffie-Hellman) cipher is used. Support is also added for the x25519 and x448 curves for TLSv1.2 handshake key exchange.

These updates also apply to TLSv1.0 and TLSv1.1.

Restriction: For TLSv1.0, TLSv1.1, and TLSv1.2, curves x25519 and x448 are not enabled by default and must be configured explicitly both for the AT-TLS client and server.

Dependencies: z/OS V2R5 System SSL APAR OA61783 is required.

Using AT-TLS support for x25519 and x448 key exchange for TLSv1.2

To use AT-TLS support for x25519 and x448 key exchange for TLSv1.2, complete the appropriate tasks in Table 35 on page 46.

Table 35. Task topics to enable AT-TLS support for x25519 and x448 key exchange for TLSv1.2	
Task	**Reference**
Understand the use of elliptic curves for a TLSv1.0-TLSv1.2 negotiation	Limiting Key Exchange Elliptic Curves for TLSv1.0, TLSv1.1, and TLSv1.2 in z/OS Communications Server: IP Configuration Guide

Table 35. Task topics to enable AT-TLS support for x25519 and x448 key exchange for TLSv1.2 (continued)	
Task	**Reference**
Configure a list of allowed elliptical curves for TLSv1.0-TLSv1.2 key exchange negotiations for an AT-TLS server.	• Online help of IBM Configuration Assistant for z/OS Communications Server • ServerKexECurves parameter on the TTLSSignatureParms statement in z/OS Communications Server: IP Configuration Reference
Configure support for elliptic curves x25519 and x448 for TLSv1.0-TLSv1.2 key exchange negotiations for an AT-TLS client.	• Online help of IBM Configuration Assistant for z/OS Communications Server • ClientECurves parameter on the TTLSSignatureParms statement in z/OS Communications Server: IP Configuration Reference
Display AT-TLS policy using the z/OS UNIX pasearch command to query information from the Policy Agent.	z/OS UNIX pasearch command: Display policies in z/OS Communications Server: IP System Administrator's Commands
Display AT-TLS policy for an active connection using the Netstat TTLS/-x command.	Netstat TTLS/-x report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about AT-TLS support for x25519 and x448 key exchange for TLSv1.2, see Table 36 on page 47.

Table 36. All related topics about AT-TLS support for x25519 and x448 key exchange for TLSv1.2	
Book name	**Topics**
z/OS Communications Server: IP Configuration Reference	TTLSSignatureParms statement
z/OS Communications Server: IP System Administrator's Commands	• Netstat TTLS/-x report • z/OS UNIX pasearch command: Display policies
z/OS Communications Server: IP Configuration Guide	Limiting Key Exchange Elliptic Curves for TLSv1.0, TLSv1.1, and TLSv1.2

Support for SMF compliance evidence

z/OS V2R5 Communications Server with APAR PH37372 generates new SMF type 1154 records that provide compliance evidence for the TCP/IP stack (subtype 1), FTP daemon (subtype 2), TN3270E Telnet server (subtype 3), and CSSMTP client (subtype 4).

This data can be helpful in determining compliance with various industry regulations and standards.

These records are generated whenever an Event Notification Facility (ENF) 86 signal is emitted by a system in the sysplex and the ENF 86 parameter list includes the local z/OS system name. The ENF 86 signal is triggered by a z/OSMF Compliance REST API.

Restriction: z/OS APARs OA61443 and OA61444 are required to support the new ENF 86 signal.

Dependencies:

- The TCP/IP stack must be active to provide the TCP/IP stack compliance evidence SMF record.
- The FTP daemon must be active to provide the FTP daemon compliance evidence SMF record.
- The TN3270E Telnet server must be active to provide TN3270E Telnet server compliance evidence SMF records (one per server port).
- CSSMTP must be active to provide the CSSMTP client compliance evidence record.

Using Support for SMF compliance evidence

To use Support for SMF compliance evidence, complete the appropriate tasks in Table 37 on page 48.

Table 37. Task topics to enable Support for SMF compliance evidence

Task	Reference
Review the data provided in the SMF 1154 records.	• SMF type 1154 records and Appendix F. Type 1154 SMF records in z/OS Communications Server: IP Programmer's Guide and Reference • Assembler mapping macro EZASM482 can be found in SYS1.MACLIB • C header mapping file can be found in SEZANMAC(EZA482) or /usr/include/eza482.h

To find all related topics about Support for SMF compliance evidence, see Table 38 on page 48.

Table 38. All related topics about Support for SMF compliance evidence

Book name	Topics
z/OS Communications Server: IP Configuration Guide	Accounting - SMF records
z/OS Communications Server: IP Programmer's Guide and Reference	• SMF records • SMF type 1154 records • Appendix F. Type 1154 SMF records
z/OS Release Upgrade Reference Summary	• New and changed System Management Facilities (SMF) records for z/OS V2R5 • New and changed members in SYS1.MACLIB for z/OS V2R5

FTP server JES access control

z/OS V2R5 Communications Server, with APAR PH42618, supports a new SAF resource in the SERVAUTH class to control which users are allowed to access FTP JES mode. When the SERVAUTH class is active and a profile is defined for the EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES SAF resource, only users with permission to the profile are allowed to access FTP JES mode.

Dependency: The SERVAUTH class must be active for the EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES SAF resource to provide access controls.

To use FTP server JES access control, complete the appropriate tasks in Table 39 on page 49.

Table 39. Task topics to enable FTP server JES access control	
Task	**Reference**
Implement FTP JES access controls using the SERVAUTH class • Activate the SERVAUTH class, if it is not already active. • Define an EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES SAF resource profile with UACC(NONE). • For each user that should be allowed to use FTP FILETYPE=JES, give the user READ permission to the defined profile.	(Optional) Steps for controlling user access to FTP JES mode in z/OS Communications Server: IP Configuration Guide

Using FTP server JES access control

To find all related topics about FTP server JES access control, see Table 40 on page 49.

Table 40. All related topics about FTP server JES access control	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Local user access control to TCP/IP resources using SAF • Security for the FTP server • (Optional) Steps for controlling user access to FTP JES mode • Customizing the FTP-to-JES interface for JESINTERFACELevel 2 (optional)
z/OS Communications Server: IP Configuration Reference	• FILETYPE (FTP client and server) statement
z/OS Communications Server: IP User's Guide and Commands	• Restricting access to FTP JES mode with SAF profiles • JES security using JESINTERFACELEVEL 2 • Changing JESSTATUS, JESOWNER, and JESJOBNAME
z/OS Communications Server: IP and SNA Codes	• 200-: User *user_name* is not allowed to use FILETYPE=JES

IBM zERT Network Analyzer passphrase and password management support

The IBM zERT Network Analyzer with APAR PH43119 for z/OS V2R5 supports the use of passphrases up to 100 characters to connect to the Db2 for z/OS database. The IBM zERT Network Analyzer includes additional enhancements in the **Database Settings** panel to clear existing database credentials to allow for easier switching to a different database user ID.

Using IBM zERT Network Analyzer passphrase and password management support

To use IBM zERT Network Analyzer passphrase and password management support, perform the tasks in Table 41 on page 50.

Table 41. IBM zERT Network Analyzer passphrase and password management support	
Task/Procedure	**Reference**
Configure the passphrase for the IBM zERT Network Analyzer database	See *Working with the Database Settings panel* of *IBM zERT Network Analyzer online help*, Analysis category under the IBM z/OS Management Facility online help
Clear the existing saved IBM zERT Network Analyzer database	See *Working with the Database Settings panel* of *IBM zERT Network Analyzer online help*, Analysis category under the IBM z/OS Management Facility online help

To find all related topics about IBM zERT Network Analyzer passphrase and password management support, see Table 42 on page 50.

Table 42. All related topics about IBM zERT Network Analyzer passphrase and password management support	
Book name	**Topics**
z/OS Management Facility online help	IBM zERT Network Analyzer online help

AT-TLS currency with System SSL

z/OS V2R5 Communications Server provides AT-TLS support for RFC 7627 "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension". RFC 7627 defines an extended master secret extension. The extension is used to negotiate whether an extended master secret computation will be used for a TLSv1.2 or earlier handshake.

Using AT-TLS currency with System SSL

Incompatibility: TLSv1.3 does not use the extended master secret extension to negotiate whether an extended master secret computation will be used or not. The same protection provided by the extended master secret computation is built into the base TLSv1.3 support.

To enable AT-TLS currency with System SSL, perform the tasks in Table 43 on page 50.

Table 43. AT-TLS currency with System SSL	
Task/Procedure	**Reference**
Review the options for enabling AT-TLS support for the Extended Master Secret extension and computation. By default, the support is enabled for AT-TLS clients and servers.	• *Network Configuration Assistant online help* • ClientExtendedMasterSecret and ServerExtendedMasterSecret parameters in TTLSEnvironmentAdvancedParms statement and TTLSConnectionAdvancedParms statement in z/OS Communications Server: IP Configuration Reference
Display AT-TLS policy using the z/OS UNIX pasearch command to query information from the Policy Agent.	The z/OS UNIX pasearch command: Display policies in z/OS Communications Server: IP System Administrator's Commands
Display AT-TLS policy for an active connection using the Netstat TTLS/-x command.	Netstat TTLS/-x report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about AT-TLS currency with System SSL, see Table 44 on page 51.

Table 44. All related topics about AT-TLS currency with System SSL	
Book name	**Topics**
z/OS Communications Server: IP System Administrator's Commands	• COnn report examples • Report field descriptions • The z/OS UNIX pasearch command: Display policies
z/OS Communications Server: IP Configuration Reference	• TTLSEnvironmentAdvancedParms statement • TTLSConnectionAdvancedParms statement • General syntax rules for Policy Agent

zERT policy-based enforcement

z/OS V2R5 Communications Server enhances the z/OS Encryption Readiness Technology (zERT) function to provide enforcement of your network encryption standards. The zERT policy-based enforcement (zERT enforcement) solution allows policy-based rules that describe different levels of cryptographic protection along with optional actions to take when TCP connections match those rules. zERT enforcement actions enable immediate notification through messages, auditing through SMF records, and automatic connection termination when questionable or unacceptable cryptographic protection is detected.

z/OS network security administrators can create and manage zERT enforcement rules and actions through the Network Configuration Assistant with APAR PH35304 and the z/OS Communications Server policy agent.

Restrictions:

- zERT enforcement applies only to TCP traffic. It does not apply to UDP traffic (including EE) or traffic using other IP protocols.
- For TLS and SSH, zERT enforcement uses the cryptographic protection attributes that are obtained through stream observation only. A limited amount of security attribute data is available through observation as compared to data obtained by zERT enabled z/OS cryptographic protocol providers.
- zERT discovery collects cryptographic security attributes for the TLS, SSL, SSH, and IPsec protocols. No other cryptographic security protocols are supported. For more information, see What are the limitations for zERT discovery? in z/OS Communications Server: IP Configuration Guide.

Dependencies:

- z/OS Encryption Readiness Technology (zERT) function must be enabled with the GLOBALCONFIG statement in the TCP/IP profile.
- To create and manage zERT enforcement rules and actions with the Network Configuration Assistant (NCA), NCA APAR PH35304 is required.
- zERT enforcement requires policy agent to be started.
- If you plan to configure zERT enforcement to log messages to syslogd, the syslog daemon and traffic regulation manager daemon (TRMD) must be active.

Using zERT policy-based enforcement

To use the zERT policy-based enforcement, perform the tasks in Table 45 on page 52.

Table 45. zERT policy-based enforcement

Task/Procedure	Reference
Evaluate zERT policy-based enforcement requirements.	• How does zERT enforcement work? in z/OS Communications Server: IP Configuration Guide • Defining a zERT enforcement policy in z/OS Communications Server: IP Configuration Guide
(Preferred) Use the IBM Configuration Assistant for z/OS Communications Server to create the zERT enforcement policies and install them on the z/OS system where policy agent can process them	*Network Configuration Assistant online help*

(Optional) To define zERT enforcement policies manually in policy agent:
• Understand the policy configuration files
• Review sample zERT enforcement policy definitions
• Enable zERT configuration for policy agent
• Create zERT enforcement rules per security protocol
	• Policy-based networking inz/OS Communications Server: IP Configuration Guide
	• Policy configuration files and Policy Agent general configuration file statements in z/OS Communications Server: IP Configuration Reference
	• ZERTConfig statement, PolicyServer statement, and DynamicConfigPolicyLoad statement in z/OS Communications Server: IP Configuration Reference
	• zERT policy statements in z/OS Communications Server: IP Configuration Reference
	• The policy agent sample file is provided here:
	`/usr/lpp/tcpip/samples/pagent.conf`
	• The ZERT policy sample file is provided here:
	`/usr/lpp/tcpip/samples/pagent_ZERT.conf`

Enable z/OS Encryption Readiness Technology discovery function	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
If an audit action is enabled in your zERT enforcement policies: • Determine where zERT SMF records are to be collected – If you want the records to go to the System Management Facility, specify SMFCONFIG TYPE119 ZERTDETAILBYPOLICY. – If you want the records to be available to the real-time NMI zERT service (SYSTCPER), specify NETMONITOR ZERTSERVICEBYPOLICY. – If you want the records available to both services, specify both SMFCONFIG TYPE119 ZERTDETAILBYPOLICY and NETMONITOR ZERTSERVICEBYPOLICY. • Use the information from the SMF 119 subtype 11 'zERT enforcement' event records that provide zERT data	• Selecting a destination for zERT discovery SMF record in z/OS Communications Server: IP Configuration Guide • SMFCONFIG statement in z/OS Communications Server: IP Configuration Reference • NETMONITOR statement in z/OS Communications Server: IP Configuration Reference • zERT connection detail record (subtype 11) in z/OS Communications Server: IP Programmer's Guide and Reference

Table 45. zERT policy-based enforcement (continued)

Task/Procedure	Reference
If a syslogd logging action is enabled in your zERT enforcement policies: • (Optional) Configure syslogd rule to direct zERT messages to a file. zERT messages are written to syslog facility local5 using the priority configured for the zERT action. • Start syslog daemon • Start TRMD (for each stack in use)	• Syslog daemon in z/OS Communications Server: IP Configuration Reference • Starting the traffic regulation manager daemon (TRMD) from the z/OS shell and Starting the traffic regulation manager daemon (TRMD) as a started task in z/OS Communications Server: IP Configuration Reference
If a console logging action is enabled in your zERT enforcement policies, to prevent the TCP/IP job log from growing very large and filling up the spool space, ensure that the TCP/IP job log is being spun-off on a regular basis.	• Writing your own master scheduler JCL in z/OS MVS Initialization and Tuning Reference • Determining the source JCL for the started task in z/OS MVS JCL Reference • JESLOG parameter in z/OS MVS JCL Reference
Start the Policy Agent	• Starting and stopping the Policy Agent in z/OS Communications Server: IP Configuration Guide • Starting Policy Agent from the z/OS shell and Starting Policy Agent as a started task in z/OS Communications Server: IP Configuration Reference
Display zERT configuration settings in the TCP/IP profile	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display zERT enforcement policy entries (rules and actions) • Issue the **pasearch -z** command	The z/OS UNIX pasearch command: Display policies in z/OS Communications Server: IP System Administrator's Commands
Display the names of the zERT enforcement policy rule for a connection • Issue the **Netstat ALL/-A** command	Netstat ALL/-A report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about zERT policy-based enforcement, see Table 46 on page 54.

Table 46. All related topics about zERT policy-based enforcement

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Logging of system messages • zERT information service access control • Secure Shell (SSH) • Monitoring cryptographic network protection: z/OS encryption readiness technology (zERT) • How does zERT discovery provide the information? • What are the limitations for zERT discovery? • What does zERT aggregation collect? • How does zERT aggregation provide the information? • How does zERT enforcement work? • Using z/OS Encryption Readiness Technology • Enabling zERT discovery • Enabling zERT policy-based enforcement • Selecting a destination for zERT discovery SMF records • Disabling zERT discovery • Defining a zERT enforcement policy • Policy types and infrastructure overview • Configuration files and policy definition files • Storing configuration files and policy definition files • TCP/IP stack • Policy Agent policies • Policy sample files • zERT policy-based enforcement (ZERT) policy • Policy configuration files • Step 1: Configure general information • Step 2: Configure Policy Agent as a policy server • Step 4: Configure policies in Policy Agent configuration files • Stopping the Policy Agent • FLUSH and PURGE considerations • Switching between local and remote policies • Traffic regulation management daemon

Table 46. All related topics about zERT policy-based enforcement (continued)

Book name	Topics
z/OS Communications Server: IP Configuration Reference	• NETMONITOR statement • SMFCONFIG statement • Policy Agent and policy applications • Policy Agent configuration files overview • Policy Agent configuration statements overview • General syntax rules for Policy Agent • PolicyServer statement • DynamicConfigPolicyLoad statement • IpAddr statement • IpAddrGroup statement • IpAddrSet statement • Facilities used by z/OS Communications Server • ZERTConfig statement • zERT policy statement
z/OS Communications Server: IP Diagnosis Guide	• Diagnosing zERT policy-based enforcement problems • Overview • Policy definition problems
z/OS Communications Server: IP System Administrator's Commands	• The z/OS UNIX pasearch command: Display policies • Netstat CONFIG/-f report – Not IPv6 enabled (SHORT format) – IPv6 enabled or request for LONG format – Report field description • Netstat ALL/-A report z/OS UNIX syntax – Not IPv6 enabled (SHORT format) – IPv6 enabled or request for LONG format – Report field description
z/OS Communications Server: IP Programmer's Guide and Reference	• Real-time TCP/IP network monitoring NMI • Real-time NMI: Interacting with the servers • Requests sent by the client to the server: SYSTCPER service • Processing the cte records for SYSTCPER • zERT connection detail record (subtype 11) • TCP connection termination record (subtype 2) • TCP/IP profile record management section
z/OS Communications Server: Quick Reference	pasearch command

Table 46. All related topics about zERT policy-based enforcement (continued)

Book name	Topics
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ8544I • EZZ8546I • EZZ8547I • EZZ8551I • EZZ8552I • EZZ8553I • EZZ8554I • EZZ8555I • EZZ8556I • EZZ8557I • EZZ8558I • EZZ8559I • EZZ8560I • EZZ8561I • EZZ8562I • EZZ8563I • EZZ8564I • EZZ8565I • EZZ8583I • EZZ8584I • EZZ8585I • EZZ8586I

AT-TLS and IPsec certificate diagnostics

z/OS V2R5 Communications Server provides additional certificate diagnostic data to allow you to more quickly determine the cause of an AT-TLS or IPsec negotiation failure. New syslogd messages are provided to identify certificate validation errors detected when processing a peer's certificate.

Restrictions:

- Certificate diagnostic messages are provided when the validation of the peer's certificate fails. For validation failures accessing the local certificate, certificate diagnostic data is not provided.
- For IPsec negotiation failures due to errors with the peer's certificate, certificate diagnostic data will only be provided when the failure is detected by System SSL.

Dependencies:

The syslog daemon (i.e. syslogd) must be active. For AT-TLS and IPsec, the additional certificate diagnostic messages are written to syslogd.

Using AT-TLS and IPsec certificate diagnostics

To enable AT-TLS and IPsec certificate diagnostics, perform the tasks in Table 47 on page 57.

Table 47. AT-TLS and IPsec certificate diagnostics

Task/Procedure	Reference
If you use AT-TLS to secure connections, view the tracing levels enabled in the AT-TLS policy. • When the trace level includes error, message "EZD2052I TTLS Certificate Diagnostics" is written to syslogd when additional certificate information is available for a negotiation failure. • When the trace level includes event, messages "EZD2053I TTLS Certificate Diagnostics Details" and "EZD2054I TTLS Certificate Diagnostics Data Sources" are written to syslogd when additional certificate information is available for a negotiation failure.	• In z/OS Communications Server: IP Configuration Reference, Trace parameter in – TTLSGroupAction statement – TTLSEnvironmentAction statement – TTLSConnectionAction statement • Rule Advanced Settings, Tracing tab in Network Configuration Assistant
If you use IPsec to secure network traffic, view the log levels enabled in the IKED configuration file. • When the log level includes level 1 (default level), message "EZD2055I Certificate Diagnostics" is written to syslogd when additional certificate information is available for a negotiation failure. • When the log level includes level 4 (debug for security association negotiations), messages "DEBUGSA : Certificate Diagnostics Details" and "DEBUGSA : Certificate Diagnostics Data Sources" are written to syslogd when additional certificate information is available for a negotiation failure.	• IkeSyslogLevel parameter in IkeConfig statement in z/OS Communications Server: IP Configuration Reference • IKE Daemon Syslog Trace in Network Configuration Assistant

To find all related topics about AT-TLS and IPsec certificate diagnostics, see Table 48 on page 57.

Table 48. All related topics about AT-TLS and IPsec certificate diagnostics

Book name	Topics
z/OS Communications Server: IP Diagnosis Guide	• Common problems • Error codes • Steps for diagnosing AT-TLS problems • AT-TLS traces • AT-TLS return codes
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD0902I • EZD1139I • EZD2052I • EZD2053I • EZD2054I • EZD2055I

IPsec certificate reporting enhancements

In V2R5, the z/OS UNIX ipsec command has been enhanced to display local and remote certificate information, such as serial number and expiration date, for phase 1 tunnels. The same certificate information is provided in the IPSec Network Management Interface (NMI) NMSec_GET_IKETUN and

NMSec_GET_IKETUNCASCADE message responses, and the SMF type 119 IPsec IKE tunnel activation (subtype 73) and tunnel deactivation (subtype 74) records.

Restriction: When using the z/OS UNIX ipsec command to retrieve phase 1 tunnel data from a remote system, both the local and remote system must be at z/OS V2R5 or later for the new certificate fields to be displayed.

Using IPsec certificate reporting enhancements

To use the IPsec certificate reporting enhancements, perform the tasks in Table 49 on page 58.

Table 49. IPsec certificate reporting enhancements

Task/Procedure	Reference
Display new certificate fields on the ipsec -k display	IKE tunnel (-k) primary option in z/OS Communications Server: IP System Administrator's Commands
Process new certificate fields in the NMsec_GET_IKETUN and NMsec_GET_IKETUNCASCADE message response	NMset_GET_IKETUN and NMset_GET_IKETUNCASCADE in z/OS Communications Server: IP Programmer's Guide and Reference
Process new certificate fields in the SMF type 119 subtype 73 (IPSec IKE tunnel activation and refresh record) and the subtype 74 (IPSec IKE tunnel deactivation and expire record).	IPSec IKE tunnel activation and refresh record (subtype 73) and IPSec IKE tunnel deactivation and expire record (subtype 74) in z/OS Communications Server: IP Programmer's Guide and Reference

To find all related topics about IPsec certificate reporting enhancements, see Table 50 on page 58.

Table 50. All related topics about IPsec certificate reporting enhancements

Book name	Topics
z/OS Communications Server: IP System Administrator's Commands	• IKE tunnel (-k) primary option report example • IKE tunnel (-k) primary option report field descriptions
z/OS Communications Server: IP Programmer's Guide and Reference	• NMset_GET_IKETUN • NMset_GET_IKETUNCASCADE • IPSec IKE tunnel activation and refresh record (subtype 73) • IPSec IKE tunnel deactivation and expire record (subtype 74)
z/OS Communications Server: IP Configuration Guide	• Displaying IKE tunnel information with the ipsec command • Displaying the quick start Security Associations

Sysplex Autonomics for IPSec

z/OS V2R5 enhances the sysplex autonomics function to monitor IPsec infrastructure. You can request that sysplex autonomics delay a TCP/IP stack from joining a sysplex group until the IPsec infrastructure is active. You can also request that sysplex autonomics monitor the IPsec infrastructure after the stack has joined the sysplex group. If monitoring the IPsec infrastructure is enabled, you are alerted with new messages when the IPsec infrastructure is not operational. You can optionally configure the TCP/IP stack

to also take a recovery action and leave the sysplex when it detects that the IPsec infrastructure is not active. This allows a backup TCP/IP stack to take over DVIPAs from the system that left the sysplex.

Restrictions:

- The monitoring of the IPsec infrastructure can only be enabled for a TCP/IP stack that is using sysplex-wide security sessions (SWSA) and has the DVIPSEC parameter configured on the IPSEC statement in the TCP/IP profile.
- While the EZBDVIPA coupling facility structure is required for IPsec sysplex-wide security associations (SWSA), the ability of the TCP/IP stack to connect to or access the EZBDVIPA structure is not monitored by sysplex autonomics for IPsec. A failure related to the EZBDVIPA structure would typically be sysplex-wide. It would not be beneficial for a TCP/IP stack to leave the sysplex for a sysplex-wide failure.
- In IPsec configurations where both a primary and backup NSSD are configured for certificate services, no monitoring of the IKED connection to NSSD is done after the TCP/IP stack joins the sysplex. See the IP Configuration Guide “Sysplex Autonomics for IPsec infrastructure” for additional information.

Incompatibilities:

- If your IPsec infrastructure includes the Network Security Services daemon (NSSD), and the IKED to NSSD connection uses a DVIPA as the source or destination IP address, the sysplex autonomics IPsec infrastructure monitoring function should not be enabled.
- If you use a centralized Policy Agent server for IPsec or AT-TLS policy, and the connection from the policy client to the policy server uses a DVIPA as the source or destination IP address, the sysplex autonomics IPsec infrastructure monitoring function should not be enabled.

Using Sysplex Autonomics for IPSec

To enable Sysplex Autonomics for IPSec, perform the tasks in Table 51 on page 59.

Table 51. Sysplex Autonomics for IPSec

Task/Procedure	Reference
Enable monitoring of the IPsec infrastructure by sysplex autonomics with the GLOBALCONFIG SYSPLEXMONITOR sub-parameters DELAYJOINIPSEC and MONIPSEC	• GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference • Sysplex problem detection and recovery topic in z/OS Communications Server: IP Configuration Guide
Display sysplex autonomics configuration settings	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
(Optional) Configure the NoKeyring parameter on the IkeConfig statement in the IKE configuration file, if appropriate. If an IKE key ring is not explicitly configured, the Keyring parameter defaults to iked/keyring. If there is no keyring for IKED to process, you can specify NoKeyring.	IkeConfig statement in z/OS Communications Server: IP Configuration Reference
Display the IKED configuration parameters	MODIFY command: IKE server in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about Sysplex Autonomics for IPSec, see Table 52 on page 60.

Table 52. All related topics about Sysplex Autonomics for IPSec	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Sysplex problem detection and recovery • Problem detection • Recovery • Summary of problems monitored and actions taken • Sysplex autonomics for IPsec
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement • IkeConfig statement
z/OS Communications Server: IP System Administrator's Commands	• Not IPv6 enabled (SHORT format) • IPv6 enabled or request for LONG format • Report field descriptions • VARY TCPIP,,SYSPLEX Parameters • Netstat CONFIG/-f report • MODIFY command: IKE server
z/OS Communications Server: IP Programmer's Guide and Reference	TCP/IP profile record Global configuration section
z/OS Communications Server: IP Diagnosis Guide	Sample output of the TCPIPCS PROFILE subcommand
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD1976E • EZD1977E • EZD1979E • EZD2048I • EZD2049I • EZD2050I
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	EZZ0839I

IBM zERT Network Analyzer database administration enhancements

z/OS Management Facility (z/OSMF) V2R5 with the IBM zERT Network Analyzer provides additional flexibility in IBM zERT Network Analyzer's Db2 for z/OS database schema definitions and reduces the access privileges required by the IBM zERT Network Analyzer's database user ID. The supplied database schema tooling now supports customized values for the database schema name, index names and even table names along with many other operational parameters that were already configurable.

Dependencies: No new dependencies are introduced. The IBM zERT Network Analyzer requires z/OSMF to be installed and a type 4 JDBC connection to Db2 for z/OS 11 or higher.

Using IBM zERT Network Analyzer database administration enhancements

To enable IBM zERT Network Analyzer database administration enhancements, perform the tasks in Table 53 on page 61.

Table 53. IBM zERT Network Analyzer database administration enhancements	
Task/Procedure	**Reference**
Stop z/OSMF if it is running	
• If you are installing the IBM zERT Network Analyzer for the first time, your Db2 for z/OS database administrator (DBA) will need to create your customized database using the provided schema tooling. • If you already have the IBM zERT Network Analyzer running: – Your DBA needs to either upgrade the existing database schema to the new schema version or else drop your existing database and re-create it with customized schema, index and/or table names at the new schema version. – Regardless of which approach you decide, your DBA uses the provided database schema tooling to implement the changes. This includes deciding on and defining the desired number of IBM zERT Network Analyzer query result table partitions.	See Db2 for z/OS customization for the IBM zERT Network Analyzer task in IBM z/OS Management Facility Configuration Guide
Once the IBM zERT Network Analyzer database is updated to or created at the new schema version , start z/OSMF and the IBM zERT Network Analyzer plugin. If you are using a newly created database, you need to fill in and save the required JDBC connectivity settings in the IBM zERT Network Analyzer's database settings panel.	See Connect the IBM zERT Network Analyzer task with the Db2 for z/OS database in IBM z/OS Management Facility Configuration Guide
Once the correct database settings are stored and the IBM zERT Network Analyzer successfully connects to the database, you can verify the database schema information in the database settings panel.	See *Working with the Database Settings panel* of IBM zERT Network Analyzer online help, *Analysis* category under the IBM z/OS Management Facility online help
(Optionally) Configure the report timeout value to specify how many minutes of inactivity will result in the report being closed and the associated query result table partition being made available for future query requests.	IBM zERT Network Analyzer online help
(Optionally) Configure the maximum number of reports a single user can have concurrently open.	IBM zERT Network Analyzer online help

To find all related topics about IBM zERT Network Analyzer database administration enhancements, see Table 54 on page 61.

Table 54. All related topics about IBM zERT Network Analyzer database administration enhancements	
Book name	**Topics**
IBM z/OS Management Facility Configuration Guide	• Updating z/OS for the IBM zERT Network Analyzer plug-in • Db2 for z/OS customization for the IBM zERT Network Analyzer task • Recovering unavailable partition

Table 54. All related topics about IBM zERT Network Analyzer database administration enhancements (continued)	
Book name	**Topics**
z/OS Management Facility online help	IBM zERT Network Analzyer online help

Application development

The following topics describe enhancements for application development:

- "SMTPD compatibility enhancements for CSSMTP" on page 62

SMTPD compatibility enhancements for CSSMTP

z/OS V2R5 Communications Server enhances the Communications Server SMTP (CSSMTP) application with three new configuration parameters to provide better compatibility with SMTPD for your migration from SMTPD to CSSMTP.

To enable SMTPD compatibility enhancements for CSSMTP, perform the tasks in Table 55 on page 62.

Using SMTPD compatibility enhancements for CSSMTP

To use the SMTPD compatibility enhancements for CSSMTP, perform the tasks in Table 55 on page 62.

Table 55. SMTPD compatibility enhancements for CSSMTP	
Task/Procedure	**Reference**
Configure ReportMailFrom to define a default email address for the "Mail From" field in the error report.	ReportMailFrom statement in Communications Server SMTP application in z/OS Communications Server: IP Configuration Reference
Configure ReportSysoutClass to assign a Sysout Class for error reports.	ReportSysoutClass statement in Communications Server SMTP application in z/OS Communications Server: IP Configuration Reference
Configure MailBoxCompatibility to define the mailbox length (Standard or Long).	MailBoxCompatibility statement in Communications Server SMTP application in z/OS Communications Server: IP Configuration Reference
Display the values for the ReportMailFrom, ReportSysoutClass, and MailBoxCompatibility.	MODIFY command: Communications Server SMTP application (CSSMTP) in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about SMTPD compatibility enhancements for CSSMTP, see Table 56 on page 62.

Table 56. All related topics about SMTPD compatibility enhancements for CSSMTP	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	Customizing the CSSMTP configuration file to handle undeliverable mail

Table 56. All related topics about SMTPD compatibility enhancements for CSSMTP (continued)

Book name	Topics
z/OS Communications Server: IP Configuration Reference	• Communications Server SMTP application – General syntax rules for CSSMTP – CSSMTP configuration statements - MailBoxCompatibility statement - ReportMailFrom statement - ReportSysoutClass statement
z/OS Communications Server: IP System Administrator's Commands	• MODIFY command: Communications Server SMTP application (CSSMTP)

Chapter 4. Communications Server interface changes for z/OS V2R5

This topic includes the Communications Server interface changes for z/OS V2R5.

In addition to the interface changes included in this topic, refer to the following topics in the z/OS V2R5 Release Upgrade Reference Summary for additional information.

- *New and changed members in SYS1.MACLIB for z/OS V2R5*
- *New and changed SYS1.PARMLIB members for z/OS V2R5*
- *New and changed System Management Facilities (SMF) records for z/OS V2R5*

The Communications Server interface changes described in this topic are:

The tables in this topic contain a **Reason for change** column that provides the name of the related functional enhancement.

Communications Server IP interface changes

This topic describes the following Communications Server IP interfaces:

PROFILE.TCPIP configuration file

This topic contains the PROFILE.TCPIP statement and parameter changes.

PROFILE.TCPIP statement and parameter changes

Table 57 on page 67 lists the new and updated Communications Server PROFILE.TCPIP configuration statements and parameters. See z/OS Communications Server: IP Configuration Reference for more detailed information.

Table 57. New and changed Communications Server PROFILE.TCPIP configuration statements and parameters for z/OS V2R5

Statement	Description	Reason for change
GLOBALCONFIG	The following new subparameter is added to the SMCGLOBAL parameter: • SMCEID/ENDSMCEID The following new subparameter is added to the SMCD parameter: • SYSTEMEID/NOSYSTEMEID The following new subparameters are added to the SMCGLOBAL parameter: • SMCPERMIT/ENDSMCPERMIT • SMCEXCLUDE/ENDSMCEXCLUDE	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GLOBALCONFIG	The following new subparameters are added to the SYSPLEXMONITOR parameter: • DELAYJOINIPSEC • MONIPSEC	Sysplex Autonomics for IPSec
GLOBALCONFIG	The following new subparameters are added to the ZERT AGGREGATION parameter: • INTVAL • SYNCVAL	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
GLOBALCONFIG	The following new parameters are added: • IKEDREQUIRED • POLICYREQUIRED	Notification of availability of TCP/IP extended services
INTERFACE	The following new subparameters are added to the SMCR parameter of the INTERFACE-IPAQENET statement: • PFID • SMCRIPADDR • SMCRMTU	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
NETMONITOR	New ZERTSERVICEBYPOLICY and NOZERTSERVICEBYPOLICY parameters are added to control creation of zERT-related SMF 119 subtype 11 records by zERT policy-based enforcement.	zERT policy-based enforcement
SMFCONFIG	New ZERTDETAILBYPOLICY and NOZERTDETAILBYPOLICY parameters are added to control creation of zERT-related SMF 119 subtype 11 records by zERT policy-based enforcement.	zERT policy-based enforcement
VIPABACKUP **VIPADEFINE**	The SERVICEMGR parameter has been removed due to deprecation of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB).	Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)

Table 57. New and changed Communications Server PROFILE.TCPIP configuration statements and parameters for z/OS V2R5 (continued)		
Statement	**Description**	**Reason for change**
VIPADISTRIBUTE	The GRE, ENCAP, TARGCONTROLLED, and CONTROLPORT parameters have been removed from the Tier1 options due to the deprecation of support for workload distribution to non-z/OS targets.	Removal of support for load balancing to Data Power®
VIPASMPARMS	The VIPASMPARMS statement has been removed due to the deprecation of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB).	Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)

Configuration files

This topic includes information about the following configuration statements and files:

- "FTP client configuration statements" on page 68
- "FTP server configuration statements" on page 68
- "TN3270E Telnet server PROFILE configuration file" on page 69
- "General updates for the non-PROFILE.TCPIP IP configuration files" on page 71

The Communications Server PROFILE.TCPIP configuration file updates are in a separate topic; see "PROFILE.TCPIP configuration file" on page 66.

See z/OS Communications Server: IP Configuration Reference for more detailed information about all of the Communications Server IP configuration files and statements.

FTP client configuration statements

Table 58 on page 68 lists the new and updated FTP client configuration statements. See *z/OS Communications Server: IP Configuration Reference* for more detailed information.

Table 58. New and changed Communications Server FTP client configuration statements for V2R5		
Statement	**Description**	**Reason for change**
TLSRFCLEVEL	CCCNONOTIFY value is no longer supported for the FTP client if TLSMECHANISM ATTLS is configured.	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

FTP server configuration statements

Table 59 on page 68 lists the new and updated FTP server configuration statements. See *z/OS Communications Server: IP Configuration Reference* for more detailed information.

Table 59. New and changed Communications Server FTP server configuration statements for z/OS V2R5		
Statement	**Description**	**Reason for change**
• **CIPHERSUITE** • **KEYRING** • **SSLV3** • **TLSTIMEOUT**	Keyword is no longer supported for the FTP server.	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

Table 59. New and changed Communications Server FTP server configuration statements for z/OS V2R5 (continued)		
Statement	**Description**	**Reason for change**
CTRL_TLS_SESSTCKTS	New statement for controlling the sending of TLSv1.3 session tickets for session reuse.	APAR PH51772
TLSRFCLEVEL	CCCNONOTIFY value is no longer supported for the FTP server.	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
TLSMECHANISM	• FTP value is no longer supported for the FTP server. • Default value changed to ATTLS for the FTP server.	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

TN3270E Telnet server PROFILE configuration file

During initialization of the TN3270E Telnet server (Telnet) address space, configuration parameters are read from a configuration PROFILE data set. The PROFILE data set is used to configure Telnet to accept or reject connection requests. You can update the PROFILE data set to change or add statements to support new functions, or to change or add usage rules.

This topic includes tables with the descriptions of the new and changed Telnet PROFILE configuration statements. See z/OS Communications Server: IP Configuration Reference for complete information on configuration statements and the PROFILE statement.

BEGINVTAM information block

There is no new and changed BEGINVTAM information block for V2R5.

TELNETGLOBALS information block

The TELNETGLOBALS information block is a Telnet configuration block used to provide definitions that apply to all Telnet ports.

Table 60. Summary of new and changed Communications Server Telnet configuration file - TELNETGLOBALS block for z/OS V2R5		
Statement	**Description**	**Reason for change**
CLIENTAUTH	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
CRLLDAPSERVER	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
ENCRYPTION	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

Table 60. Summary of new and changed Communications Server Telnet configuration file - TELNETGLOBALS block for z/OS V2R5 (continued)		
Statement	**Description**	**Reason for change**
KEYRING	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
SSLTIMEOUT	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
SSLV2 and NOSSLV2	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
SSLV3 and NOSSLV3	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

TELNETPARMS information block

Table 61. Summary of new and changed Communications Server Telnet configuration file - TELNETPARMS block for z/OS V2R5		
Statement	**Description**	**Reason for change**
SECUREPORT	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
CLIENTAUTH	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
CRLLDAPSERVER	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
ENCRYPTION	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

Table 61. Summary of new and changed Communications Server Telnet configuration file - TELNETPARMS block for z/OS V2R5 (continued)

Statement	Description	Reason for change
KEYRING	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
SSLTIMEOUT	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
SSLV2 and NOSSLV2	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
SSLV3 and NOSSLV3	Keyword no longer supported for the TN3270E Telnet server	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

General updates for the non-PROFILE.TCPIP IP configuration files

Table 62 on page 72 lists the general updates for the Communications Server IP configuration files.

Table 62. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R5

File	Statement / Entry	Description	Reason for change
AT-TLS policy files	• TTLSEnvironmentAdvancedParms • TTLSConnectionAdvancedParms	New parameters, ClientExtendedMasterSecret and ServerExtendedMasterSecret, are defined for each statement.	AT-TLS currency with System SSL
	• TTLSEnvironmentAdvancedParms • TTLSConnectionAdvancedParms	New parameters HostReferenceIdDNS, HostReferenceIdCN, and HostRefWildcardValidation	AT-TLS currency with System SSL
	TTLSGskAdvancedParms	New parameter GSK_SYSPLEX_SESSION_TICKET_CACHE and GSK_SESSION_TICKET_CLIENT_MAXCACHED	
	TTLSSignatureParms	• New parameter ServerKexECurves • New values x25519 and x448 on the ClientECurves parameter	AT-TLS support for x25519 and x448 key exchange for TLSv1.2
DCAS configuration file	KEYRING	Keyword is no longer supported	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
	LDAPPORT	Keyword is no longer supported	
	LDAPSERVER	Keyword is no longer supported	
	SAFKEYRING	Keyword is no longer supported	
	STASHFILE	Keyword is no longer supported	
	TLSV1ONLY	Keyword is no longer supported	
	V3CIPHER	Keyword is no longer supported	
	TLSMECHANISM	DCAS value is no longer supported. Default value changed to ATTLS.	

Table 62. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R5 (continued)			
File	**Statement / Entry**	**Description**	**Reason for change**
Communications Server SMTP (CSSMTP) configuration file	ReportMailFrom	New parameter ReportMailFrom is an optional parameter that specifies the mailbox to use in the Mail From field in error reports.	SMTPD compatibility enhancements for CSSMTP
	ReportSysoutClass	New parameter ReportSysoutClass is an optional parameter that specifies the SYSOUT class used for error reports.	SMTPD compatibility enhancements for CSSMTP
	MailBoxCompatibility	New parameter MailBoxCompatibility is an optional parameter to state the size of the mail box (Standard 64 characters or Long 256 characters).	SMTPD compatibility enhancements for CSSMTP
IKE daemon configuration file	New parameter NoKeyRing on the existing IkeConfig statement	NoKeyRing can be specified when no IKED key ring is provided.	Sysplex Autonomics for IPSec
Syslog daemon configuration file	The destination specification in the rule	A new -A option is provided to specify the destination IP address or hostname, the protocol (TCP or UDP), the destination port,and the TCP secure (yes or no) setting.	z/OS UNIX syslogd support for secure logging over TCP

RACF interfaces

Table 63 on page 73 lists the functions for which new or changed RACF support is available. Sample RACF commands to change the RACF configuration can be found in one of the following members of the installation data set, SEZAINST:

- EZARACF - Contains sample commands for environments where multilevel security is not configured.
- EZARACFM - Contains sample commands for environments where multilevel security is configured.

You can use the function name from the table to search EZARACF for all the commands necessary for the function. See z/OS Communications Server: IP Configuration Guide for more information for each function.

Table 63. New and changed Communications Server RACF interfaces for z/OS V2R5		
Function name	**Description**	**Reason for change**
EZB.PAGENT.sysname.imagename.ZERT	New SAF resource to control access to zERT policy for a policy client.	zERT policy-based enforcement
EZB.FTP.*sysname.ftpdaemonname*.ACCESS.JES	New SAF resource defined in the SERVAUTH class	FTP server JES access control

Operator commands

This topic includes information about the following Communications Server IP operator commands:

- "Netstat operator commands (DISPLAY TCPIP,,NETSTAT)" on page 74
- "TN3270E Telnet server operator commands" on page 77
- "General updates of IP operator commands" on page 77

See z/OS Communications Server: IP System Administrator's Commands for more detailed information.

Netstat operator commands (DISPLAY TCPIP,,NETSTAT)

Table 64 on page 74 lists the new and updated Communications Server IP Netstat operator command DISPLAY TCPIP,,NETSTAT. See Table 65 on page 77 for the other Communications Server IP operator command entries.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server IP operator commands.

All parameters in the following table are for the DISPLAY TCPIP,,NETSTAT operator command.

Table 64. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R5

Parameters	Description	Reason for change
ALL	The following information is now displayed under the SMC INFORMATION section: • SMCDVERSION • SMCEID SMCRSTATUS is now either SMCRV1STATUS or SMCRV2STATUS, depending on the SMC version. SMCDSTATUS is now either SMCDV1STATUS or SMCDV2STATUS, depending on the SMC version. Up to four status fields might be displayed now. If there is a global reason for SMC not being used, this field will be simply SMCSTATUS.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
ALL	Displays zERT enforcement policy rules in use by TCP connections.	zERT policy-based enforcement
ARP	Netstat ARP will now show ARP cache entries related to SMC-Rv2 indirect links.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
CONFIG	Displays new ZERT Aggregation sub parameter information with INTVAL and SYNCVAL in the GLOBALCONFIG section.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
CONFIG	The configured values for POLICYREQUIRED and IKEDREQUIRED are listed in the GLOBALCONFIG section.	Notification of availability of TCP/IP extended services

Table 64. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R5 (continued)

Parameters	Description	Reason for change
CONFIG	The configured SMCEIDs are listed in the SMCGlobal section. Whether a SMCDSYSEID is configured and its value, if configured, is displayed in the SMCD section. The configured SMCPERMIT entries are listed in the SMCGlobal section. The configured SMCEXCLUDE entries are listed in the SMCGlobal section.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
CONFIG	The Global Configuration Information section of the display includes the new Sysplex Monitor settings - DelayJoinIpsec and MonIpsec.	Sysplex Autonomics for IPSec
CONFIG	• Displays new ZertDetailByPolicy subparameter information in the SMFCONFIG section. • Displays new ZertSrvByPolicy subparameter information in the NETMONITOR section.	zERT policy-based enforcement
DEvlinks	The card generation level and speed information are displayed for RNIC interfaces representing "RoCE Express3" features.	Communications Server support for RoCE Express3

Table 64. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R5 (continued)

Parameters	Description	Reason for change
DEvlinks	Specifying PNETID=NONE will display all SMC-D capable interfaces without a PNETID. Specifying PNETID=* will display all SMC-D capable interfaces without a PNETID under a new PNETID=*NONE* heading. Specifying an INTFNAME of an SMC-D capable interface will display any unassociated ISM interfaces. Specifying SMC will display the following information under the SMCD LINK INFORMATION section: • SMCDversion • SMCEID, if SMCv2 • Remote host, if SMCv2 and available • Remote host type, if SMCv2 and available Specifying INTFN=osa_interface will show SMCR version capabilities of the OSA interface and the RNIC interfaces associated with those capabilities. New interface parameters PFID, SMCRIPADDR, and SMCRMTU will be displayed if configured. Specifying INTFN=rnic_interface will show SMCR version capabilities of the RNIC interface. For SMC-Rv2, this includes the IP address associated with the RNIC. Specifying PNETID=pnetid will show the new interface parameters, PFID, SMCRIPADDR, and SMCRMTU, if configured. Specifying SMC will display the following information in the SMC Link section if the link is for SMC-Rv2: • Link type: Direct or Indirect • Link role: Server or Client • If Link type is Indirect, it also shows Next Hop IP address and Next Hop MAC address Specifying SMC will display the following information in the SMC Link Group section: • SMC version • SMCEID, if SMCv2 • Remote host name, if SMCv2 and available • Remote host type, if SMCv2 and available • PNETID only displays if SMCv1	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

Table 64. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R5 (continued)		
Parameters	**Description**	**Reason for change**
TTLS CONN DETAIL	The new parameters, ClientExtendedMasterSecret and ServerExtendedMasterSecret, are displayed for the environment action and the connection action, if configured.	AT-TLS currency with System SSL
TTLS CONN DETAIL	The new parameters, GSK_SYSPLEX_SESSION_TICKET_CACHE and GSK_SESSION_TICKET_CLIENT_MAXCACHED, are displayed for the environment action, if configured. The new parameters, HostReferenceIdDNS, HostReferenceIdCN, and HostRefWildcardValidation are displayed if configured for the environment and connection action.	AT-TLS currency with System SSL
TTLS CONN DETAIL	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2
VIPADCFG	The "SrvMgr" field is no longer displayed.	Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)

TN3270E Telnet server operator commands

There are no new or changed TN3270E Telnet server operator commands for z/OS V2R5.

General updates of IP operator commands

Table 65 on page 77 lists the new and updated Communications Server IP operator commands, **except** the Netstat operator command DISPLAY TCPIP,,NETSTAT and the Telnet operator commands. See the following tables for those commands:

- Table 64 on page 74, IP Netstat operator commands (DISPLAY TCPIP,,NETSTAT)
- "TN3270E Telnet server operator commands" on page 77, Telnet operator commands

Table 65. New and changed Communications Server operator commands for z/OS V2R5			
Command	**Parameters**	**Description**	**Reason for change**
DISPLAY TCPIP	OSAINFO	New fields "EIB enabled" and "Port packet drops" added to the display.	OSA-Express Enhanced Inbound Blocking (EIB)
MODIFY CSSMTP	DISPLAY,CONFIG	Display the new values for ReportMailFrom, ReportSysoutClass, and MailBoxCompatibility statements	SMTPD compatibility enhancements for CSSMTP
MODIFY IKED	DISPLAY	Display includes the NoKeyRing parameter if configured.	Sysplex Autonomics for IPSec
VARY TCPIP	PURGECACHE	Vary PURGECACHE is enhanced to accept an RNIC interface as an input.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

TSO commands

This topic includes information about the following TSO commands:

- "NETSTAT TSO commands" on page 78
- "FTP TSO and z/OS UNIX commands" on page 81

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server TSO commands.

NETSTAT TSO commands

Table 66 on page 78 lists the new and updated Communications Server NETSTAT TSO command.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server TSO commands.

Table 66. New and changed Communications Server NETSTAT TSO commands for z/OS V2R5

Parameter	Description	Reason for change
ALL	The following information is displayed under the SMC INFORMATION section: • SMCDVERSION • SMCEID SMCRSTATUS is now either SMCRV1STATUS or SMCRV2STATUS, depending on the SMC version. SMCDSTATUS is now either SMCDV1STATUS or SMCDV2STATUS, depending on the SMC version. Up to four status fields might be displayed now. If there is a global reason for SMC not being used, this field will be simply SMCSTATUS.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
ALL	Displays zERT enforcement policy rules in use by TCP connections.	zERT policy-based enforcement
ARP	Netstat ARP will now show ARP cache entries related to SMC-Rv2 indirect links.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
CONFIG	The configured values for POLICYREQUIRED and IKEDREQUIRED are listed in the GLOBALCONFIG section.	Notification of availability of TCP/IP extended services
CONFIG	The configured SMCEIDs are listed in the SMCGlobal section. Whether a SMCDSYSEID is configured and its value, if configured, is displayed in the SMCD section. The configured SMCPERMIT entries are listed in the SMCGlobal section. The configured SMCEXCLUDE entries are listed in the SMCGlobal section.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

Table 66. New and changed Communications Server NETSTAT TSO commands for z/OS V2R5 (continued)		
Parameter	**Description**	**Reason for change**
CONFIG	The Global Configuration Information section of the display includes the new Sysplex Monitor settings - DelayJoinIpsec and MonIpsec.	Sysplex Autonomics for IPSec
CONFIG	Displays new ZERT Aggregation subparameter information with INTVAL and SYNCVAL in the GLOBALCONFIG section.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
CONFIG	• Displays new ZertDetailByPolicy subparameter information in the SMFCONFIG section. • Displays new ZertSrvByPolicy subparameter information in the NETMONITOR section.	zERT policy-based enforcement
DEvlinks	The card generation level and speed information are displayed for RNIC interfaces representing "RoCE Express3" features.	Communications Server support for RoCE Express3

Table 66. New and changed Communications Server NETSTAT TSO commands for z/OS V2R5 (continued)		
Parameter	**Description**	**Reason for change**
DEvlinks	Specifying PNETID=NONE will display all SMC-D capable interfaces without a PNETID. Specifying PNETID=* will display all SMC-D capable interfaces without a PNETID under a new PNETID=*NONE* heading. Specifying INTFNAME of an SMC-D capable interface will display any unassociated ISM interfaces. Specifying SMC will display the following information under the SMCD LINK INFORMATION section: • SMCDversion • SMCEID, if SMCv2 • Remote host, if SMCv2 and available • Remote host type, if SMCv2 and available Specifying INTFN=osa_interface will show SMCR version capabilities of the OSA interface and the RNIC interfaces associated with those capabilities. New interface parameters PFID, SMCRIPADDR, and SMCRMTU will be displayed if configured. Specifying INTFN=rnic_interface will show SMCR version capabilities of the RNIC interface. For SMC-Rv2, this includes the IP address associated with the RNIC. Specifying PNETID=pnetid will show the new interface parameters, PFID, SMCRIPADDR, and SMCRMTU, if configured. Specifying SMC will display the following information in the SMC Link section if the link is for SMC-Rv2: • Link type: Direct or Indirect • Link role: Server or Client • If Link type is Indirect, it also shows Next Hop IP address and Next Hop MAC address Specifying SMC will display the following information in the SMC Link Group section: • SMC version • SMCEID, if SMCv2 • Remote host name, if SMCv2 and available • Remote host type, if SMCv2 and available • PNETID only displays if SMCv1	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

Table 66. New and changed Communications Server NETSTAT TSO commands for z/OS V2R5 (continued)		
Parameter	**Description**	**Reason for change**
TTLS CONN DETAIL	The new parameters, ClientExtendedMasterSecret and ServerExtendedMasterSecret, are displayed for the environment action and the connection action, if configured.	AT-TLS currency with System SSL
TTLS CONN DETAIL	The new parameters, GSK_SYSPLEX_SESSION_TICKET_CACHE and GSK_SESSION_TICKET_CLIENT_MAXCACHED, are displayed for the environment action, if configured. The new parameters, HostReferenceIdDNS, HostReferenceIdCN, and HostRefWildcardValidation are displayed if configured for the environment and connection action.	AT-TLS currency with System SSL
TTLS CONN DETAIL	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2
VIPADCFG	The "SrvMgr" field is no longer displayed.	Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)

FTP TSO and z/OS UNIX commands

There are no new or changed FTP TSO and z/OS UNIX commands for z/OS V2R5.

FTP subcommands

There are no new or changed FTP subcommands for z/OS V2R5.

General updates of TSO commands

There are no general updates of TSO commands for z/OS V2R5.

z/OS UNIX commands

"General updates of z/OS UNIX commands" on page 85 lists the new and updated z/OS UNIX commands, except the z/OS UNIX FTP commands, and the z/OS UNIX netstat commands. See the following tables for those commands:

- "FTP subcommands" on page 81, FTP TSO and z/OS UNIX commands
- Table 67 on page 82, z/OS UNIX netstat commands

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server UNIX commands.

Netstat UNIX commands

Table 67 on page 82 lists the new and updated Communications Server z/OS UNIX netstat command. See "General updates of z/OS UNIX commands" on page 85 for the other (the non-netstat) z/OS UNIX command entries.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the z/OS UNIX commands.

All parameters in the following table are for the z/OS UNIX netstat command.

Table 67. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R5

Parameter	Description	Reason for change
-A	The following information is displayed under the SMC INFORMATION section: • SMCDVERSION • SMCEID SMCRSTATUS is now either SMCRV1STATUS or SMCRV2STATUS, depending on the SMC version. SMCDSTATUS is now either SMCDV1STATUS or SMCDV2STATUS, depending on the SMC version. Up to four status fields might be displayed now. If there is a global reason for SMC not being used, this field will be simply SMCSTATUS.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
-A	Displays zERT enforcement policy rules in use by TCP connections.	zERT policy-based enforcement
-d	The card generation level and speed information are displayed for RNIC interfaces representing "RoCE Express3" features.	Communications Server support for RoCE Express3

Table 67. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R5 (continued)

Parameter	Description	Reason for change
-d	Specifying PNETID=NONE will display all SMC-D capable interfaces without a PNETID. Specifying PNETID=* will display all SMC-D capable interfaces without a PNETID under a new PNETID=*NONE* heading. Specifying INTFNAME of an SMC-D capable interface will display any unassociated ISM interfaces. Specifying SMC will display the following information under the SMCD LINK INFORMATION section: • SMCDversion • SMCEID, if SMCv2 • Remote host, if SMCv2 and available • Remote host type, if SMCv2 and available Specifying INTFN=osa_interface will show SMCR version capabilities of the OSA interface and the RNIC interfaces associated with those capabilities. New interface parameters PFID, SMCRIPADDR, and SMCRMTU will be displayed if configured. Specifying INTFN=rnic_interface will show SMCR version capabilities of the RNIC interface. For SMC-Rv2, this includes the IP address associated with the RNIC. Specifying PNETID=pnetid will show the new interface parameters, PFID, SMCRIPADDR, and SMCRMTU, if configured. Specifying SMC will display the following information in the SMC Link section if the link is for SMC-Rv2: • Link type: Direct or Indirect • Link role: Server or Client • If Link type is Indirect, it also shows Next Hop IP address and Next Hop MAC address Specifying SMC will display the following information in the SMC Link Group section: • SMC version • SMCEID, if SMCv2 • Remote host name, if SMCv2 and available • Remote host type, if SMCv2 and available • PNETID only displays if SMCv1	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

Table 67. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R5 (continued)

Parameter	Description	Reason for change
-f	• Displays new ZertDetailByPolicy subparameter information in the SMFCONFIG section. • Displays new ZertSrvByPolicy subparameter information in the NETMONITOR section.	zERT policy-based enforcement
-f	Displays new ZERT Aggregation sub parameter information with INTVAL and SYNCVAL in the GLOBALCONFIG section.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
-f	The configured values for POLICYREQUIRED and IKEDREQUIRED are listed in the GLOBALCONFIG section.	Notification of availability of TCP/IP extended services
-f	The configured SMCEIDs are listed in the SMCGlobal section. Whether a SMCDSYSEID is configured and its value, if configured, is displayed in the SMCD section. The configured SMCPERMIT entries are listed in the SMCGlobal section. The configured SMCEXCLUDE entries are listed in the SMCGlobal section.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
-f	The Global Configuration Information section of the display includes the new Sysplex Monitor settings - DelayJoinIpsec and MonIpsec.	Sysplex Autonomics for IPSec
-R	Netstat ARP will now show ARP cache entries related to SMC-Rv2 indirect links.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
-x CONN DETAIL	The new parameters, ClientExtendedMasterSecret and ServerExtendedMasterSecret, are displayed for the environment action and the connection action, if configured.	AT-TLS currency with System SSL
–x CONN DETAIL	The new parameters, GSK_SYSPLEX_SESSION_TICKET_CACHE and GSK_SESSION_TICKET_CLIENT_MAXCACHED, are displayed for the environment action, if configured The new parameters, HostReferenceIdDNS, HostReferenceIdCN, and HostRefWildcardValidation are displayed if configured for the environment and connection action.	AT-TLS currency with System SSL

Table 67. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R5 (continued)		
Parameter	**Description**	**Reason for change**
–x CONN DETAIL	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2
VIPADCFG	The "SrvMgr" field is no longer displayed.	Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)

General updates of z/OS UNIX commands

Table 68 on page 85 lists the new and updated Communications Server z/OS UNIX non-netstat command.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the z/OS UNIX commands.

All parameters in the following table are for the z/OS UNIX non-netstat command.

Table 68. New and changed Communications Server z/OS UNIX commands for z/OS V2R5			
Command	**Parm**	**Description**	**Reason for change**
ipsec	-k display	This ipsec command display now includes the following new certificate details: • LocalCertExpires • LocalSerialNumber • LocalIssuerDNLength • LocalIssuerDN • LocalSubjectDNLength • LocalSubjectDN • RemoteCertExpires • RemoteSerialNumber • RemoteIssuerDNLength • RemoteIssuerDN • RemoteSubjectDNLength • RemoteSubjectDN	IPsec certificate reporting enhancements
pasearch	-z	New ZERT policy configuration displayed.	zERT policy-based enforcement
pasearch	-t	The new parameters, ClientExtendedMasterSecret and ServerExtendedMasterSecret, are displayed for the environment action and the connection action, if configured.	AT-TLS currency with System SSL

Table 68. New and changed Communications Server z/OS UNIX commands for z/OS V2R5 (continued)

Command	Parm	Description	Reason for change
pasearch	-t	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2
pasearch	-t	The new parameters, GSK_SYSPLEX_SESSION_TICKET_CACHE and GSK_SESSION_TICKET_CLIENT_MAXCACHED, are displayed for the environment action, if configured. The new parameters, HostReferenceIdDNS, HostReferenceIdCN, and HostRefWildcardValidation are displayed if configured for the environment and connection action.	AT-TLS currency with System SSL
syslogd	Start options	New options: • -T indicates that a TCP listening socket should be opened to receive messages from a remote syslogd client in the clear • -S indicates that a TCP listening socket should be opened to receive secure messages from a remote syslogd client • -U indicates that a UDP socket should be opened to receive messages from a remote syslogd	z/OS UNIX syslogd support for secure logging over TCP

Application programming interfaces and network management interfaces

This topic includes updates made to the application programming interfaces (APIs) and network management interfaces (NMIs) documented in z/OS Communications Server: IP Programmer's Guide and Reference. The following programming interfaces were updated:

- "FTP client API FCAI control block" on page 87
- "FTP client API for REXX predefined variables" on page 87
- "Local IPSec NMI" on page 87
- "Network security services NMI" on page 87
- "Real-time application-controlled TCP/IP trace NMI (EZBRCIFR)" on page 87
- "Real-time network monitoring TCP/IP NMI" on page 87
- "Resolver callable NMI (EZBREIFR)" on page 88
- "SNMP manager API" on page 88
- "Syslog daemon name/token pair" on page 88
- "TCP/IP callable NMI (EZBNMIFR)" on page 88
- "Trace formatting NMI (EZBCTAPI)" on page 90
- "Trusted TCP connections API for Java" on page 90

See z/OS Communications Server: IP Programmer's Guide and Reference for more detailed API information.

FTP client API FCAI control block

There is no new or changed FTP client API FCAI control block for z/OS V2R5.

FTP client API for REXX predefined variables

There is no new or changed FTP client API for REXX predefined variable for z/OS V2R5.

Local IPSec NMI

Table 69 on page 87 lists the updates to the Communications Server application interface for local IPSec network management interface (NMI).

Table 69. New Communications Server IP Local IPSec NMI for z/OS V2R5

Request / Response	Description	Reason for change
• **NMsec_GET_IKETUN** • **NMsec_GET_IKETUNCASCADE**	Includes the following new phase 1 IKE Tunnel data fields: • NMsIKETunLclNotAfterType • NMsIKETunLclCertExp • NMsIKETunLclSerialNumber • NMsIKETunLclSerialNumLen • NMsIKETunRmtNotAfterType • NMsIKETunRmtCertExp • NMsIKETunRmtSerialNumber • NMsIKETunRmtSerialNumLen Includes 4 new section descriptors for: • Local issuer distinguished name • Remote issuer distinguished name • Local subject distinguished name • Remote subject distinguished namec	IPsec certificate reporting enhancements

Network security services NMI

There is no new or changed Network security services NMI for z/OS V2R5.

Real-time application-controlled TCP/IP trace NMI (EZBRCIFR)

There is no new or changed Real-time application-controlled TCP/IP trace NMI (EZBRCIFR) for z/OS V2R5.

Real-time network monitoring TCP/IP NMI

Table 70 on page 87 lists the updates to the Communications Server real-time TCP/IP network monitoring NMI. For changes to SMF 119 records provided by the real-time SMF data NMI (SYSTCPSM) and the real-time TCP connection SMF data NMI (SYSTCPCN), see “SMF record type 119 enhancements” on page 94.

Table 70. New Communications Server real-time TCP/IP NMI for z/OS V2R5

NMI	Request/response	Description	Reason for change
Real-time TCP connection SMF NMI (SYSTCPCN)	TCP connection termination record (subtype 2)	New value SMF119AP_TTTermCode_Enforcement (x'77') in the SMF119AP_TTTermCode field. Indicates the connection was reset by zERT enforcement policy action.	zERT policy-based enforcement

Table 70. New Communications Server real-time TCP/IP NMI for z/OS V2R5 (continued)			
NMI	**Request/response**	**Description**	**Reason for change**
Real-time zERT SMF NMI (SYSTCPER)	zERT connection detail record (subtype 11)	• New event type SMF119SC_SAType_Enforcement (x'07') in the SMF119SC_SAEvent_Type field. Indicates the connection matches zERT enforcement policy rule with audit action. • New value SMF119SC_SAEnforcement (x'20') in the SMF119SC_SAFlags field. Indicates the connection was reset by zERT enforcement policy action. • New zERT policy-based enforcement section. Indicates the zERT enforcement policy rules in use by the TCP connection.	zERT policy-based enforcement

Resolver callable NMI (EZBREIFR)

There is no new or changed Resolver callable NMI (EZBREIFR) for z/OS V2R5.

SNMP manager API

There is no new or changed SNMP manager API for z/OS V2R5.

Syslog daemon name/token pair

There is no new or changed syslog daemon name/token pair for z/OS V2R5

TCP/IP callable NMI (EZBNMIFR)

Table 71 on page 88 lists the updates to the Communications Server TCP/IP callable NMI.

Table 71. New Communications Server TCP/IP callable NMI (EZBNMIFR) for z/OS V2R5			
Request	**Parameter/output**	**Description**	**Reason for change**
GetConnectionDetail	• NWMConnSMCVersion • NWMConnSMCEID	These new fields indicate the SMC characteristics of the connection.	Shared Memory Communications multiple IP subnet support (SMCv2)
GetConnectionDetail	• NWMConnSMCRv2Reason • NWMConnSMCDv2Reason	This new field indicates the reason SMC-Rv2 was not chosen. This new field indicates the reason SMC-Dv2 was not chosen.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GetIfs	• NWMIfSMCRStatus • NWMIfSMCDStatus • NWMIfSmcrV2_Pfid • NWMIfSmcrV2_Mtu • NWMIfSmcrV2_IpAddr	• – The following values are obsolete from the NWMIfSMCRStatus field: - NWMIFSMCRNOPNETID - NWMIFSMCRNOGC - NWMIFSMCRNOSUBMSK • – The following values are obsolete from the NWMIfSMCDStatus field: - NWMIFSMCDNOPNETID - NWMIFSMCDNOGC - NWMIFSMCDNOSUBMSK - NWMIFSMCDPNETIDMISCFG These new fields represent new INTERFACE parameters for SMC-Rv2.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

Table 71. New Communications Server TCP/IP callable NMI (EZBNMIFR) for z/OS V2R5 (continued)

Request	Parameter/output	Description	Reason for change
GetProfile	• NMTP_GBCFPolicyReq – NMTP_GBCFPolicyReq_YESIFTTLS – NMTP_GBCFPolicyReq_YES – NMTP_GBCFPolicyReq_NO • NMTP_GBCFIkedReq – NMTP_GBCFIkedReq_YESIFDYNIPSEC – NMTP_GBCFIkedReq_NO	These new fields indicate the settings of the new GLOBALCONFIG POLICYREQUIRED and IKEREQUIRED parameters.	Notification of availability of TCP/IP extended services
GetProfile	• NMTP_GBCFSYSTEMEID • NMTP_GBCFSYSTEMEIDSTR • NMTP_GBCFSMCEID • NMTP_GBCFSMCEIDCount • NMTP_GBCFUEIDList	These new fields indicate the settings of the new GLOBALCONFIG parameters.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GetProfile	• NMTP_INTFSmcrV2Pfid • NMTP_INTFSmcrV2MTU • NMTP_INTFSmcrV2IpAddr	These new NMTP_INTF fields represent new INTERFACE parameters for SMC-Rv2.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GetProfile	• NMTP_PICOSecChanged • NMTP_PICOSECFLTP • NMTP_PICOSECFLTE	New flags that indicate Permit filter section or Exclude filter section were changed. These flags are set only if the record was created due to a profile change.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GetProfile	New NMTP_FLTP and NMTP_FLTE sections: • NMTP_FLTPEye • NMTP_FLTPIPaddrV6 • NMTP_FLTPPrefix • NMTP_FLTPFLG - has the flag bit NMTP_FLTP_IPv6 to indicate if the IP address is IPv6 or IPv4 • NMTP_FLTEEye • NMTP_FLTEIPaddrV6 • NMTP_FLTEPrefix • NMTP_FLTEFLG - has the flag bits NMTP_FLTP_IPv6 to indicate if the IP address is IPv6 or IPv4	These new sections represent the configured GLOBALCONFIG SMCGLOBAL SMCPERMIT and SMCEXCLUDE lists.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GetProfile	Global configuration section: • NMTP_GBCFZERTINTV • NMTP_GBCFZERTSYNC	• New NMTP_GBCFZERTINTV flag bit that indicates the setting of the INTVAL sub-parameter on the GLOBALCONFIG statement. • New NMTP_GBCFZERTSYNC flag bit that indicates the setting of the SYNCVAL sub-parameter on the GLOBALCONFIG statement.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
GetProfile	Global configuration section: • NMTP_GBCFSysMonDelayJoinI • NMTP_GBCFSysMonIpsec	New fields, NMTP_GBCFSysMonDelayJoinI and NMTP_GBCFSysMonIpsec, indicate the settings of the new SYSPLEXMONITOR subparameters	Sysplex Autonomics for IPSec
GetProfile	Management section: • NMTP_MGMTSmf119Types • NMTP_MGMTNetMonServices	• New NMTP_MGMT119ZertDetailPolicy flag bit is set in the NMTP_MGMTSmf119Types field to indicate that the ZERTDETAILBYPOLICY parameter was specified on the SMFCONFIG TYPE119 profile statement. • NMTP_MGMTNMZertServP flag bit is set in the NMTP_MGMTNetMonServices field to indicate that the ZERTSERVICEBYPOLICY parameter was specified on the NETMONITOR profile statement.	zERT policy-based enforcement

Table 71. New Communications Server TCP/IP callable NMI (EZBNMIFR) for z/OS V2R5 (continued)			
Request	**Parameter/output**	**Description**	**Reason for change**
GetRnics	NWMRnicBGen	Value of NWMRNICBGENREXP3 represents the RoCE Express3 feature.	Communications Server support for RoCE Express3
GetRnics	• NWMRnicSmcrV2MultiIpAddr • NWMRnicSmcCapability • NWMRnicSmcrV2_MTU • NWMRnicSmcrV2IpAddr	These new fields indicate SMC characteristics of the associated RNIC.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GetSmcLinks	• NWMSmcGrp_SmcrVersion • NWMSmcGrp_Smceid • NWMSmcGrp_RemoteHostType • NwmSmcGrp_RemoteHostName • NWMSmcLnkTypeDirect • NWMSmcLnkRoleServer • NWMSmcLnkNextHopMAC • NWMSmcLnkNextHopIpAddr	These new fields indicate the SMC characteristics of the SMCD link.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
GetSmcDLinks	• NWMSmcDLnkSMCEID • NWMSmcDLnkVersion • NWMSmcDLnkRemoteOSType • NWMSmcDLnkRmtHostName	These new fields indicate the SMC characteristics of the SMCD link.	Shared Memory Communications multiple IP subnet support (SMCv2)
GetStorageStatistics	• NWMStgFlags – NWMStgZAGGCfg • New ZERT aggregation storage utilization fields – NWMStg64ZaggCurrent – NWMStg64ZaggMax	• New flag bit NWMStgZaggCfg indicates whether ZERT AGGREGATION is configured on the GLOBALCONFIG statement. • New fields NWMStg64ZaggCurrent and NWMStg64ZaggMax provide current and maximum storage usage statistics for ZERT AGGREGATION.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval

Trace formatting NMI (EZBCTAPI)

There is no new or changed trace formatting NMI (EZBCTAPI) for z/OS V2R5.

Trusted TCP connections API for Java

There is no new or changed trusted TCP connections API for Java™ for z/OS V2R5.

General updates of other NMI or API

Table 72 on page 90 lists the new and updated NMI or API.

Table 72. New and changed Communications Server NMI or API for z/OS V2R5			
Socket API	**Function call/Parameter**	**Description**	**Reason for change**
Application data: **FTP server application data format for the control connection and FTP server application data format for the data connection.**	The security method used for the FTP connection if security protection is either Private or Safe.	Value "F – TLS managed by FTP" removed.	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

Environment variables

Table 73 on page 91 lists the new and updated Communications Server environment variables. See *z/OS Communications Server: IP Configuration Reference* for more detailed information.

Table 73. New and changed Communications Server environment variables for z/OS V2R5

Environment Variables	Appl	Description	Reason for change
SYSLOGD_TCPTHREADPOOL_SIZE	Syslog daemon	New environment variable to control the size of the syslogd TCP thread pool.	z/OS UNIX syslogd support for secure logging over TCP

Socket APIs

This topic includes information about Communications Server socket APIs.

Refer to the following documents for more information about socket APIs:

- For complete documentation of the z/OS UNIX C sockets APIs, refer to z/OS XL C/C++ Runtime Library Reference
- For information about z/OS UNIX Assembler Callable Services, refer to z/OS UNIX System Services Programming: Assembler Callable Services Reference
- For information about TCP/IP socket APIs, refer to z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference
- For information about TCP/IP CICS sockets, refer to z/OS Communications Server: IP CICS Sockets Guide

General updates of socket APIs

There are no general updates of socket APIs for z/OS V2R5.

IPCS subcommands

This topic includes information about these IPCS subcommands:

See z/OS Communications Server: IP Diagnosis Guide for more detailed IPCS subcommands information.

CTRACE COMP(SYSTCPDA) subcommand

This topic lists changes to Communications Server CTRACE COMP(SYSTCPDA) subcommand options for z/OS V2R5.

There is no new or changed CTRACE COMP(SYSTCPDA) subcommand option for z/OS V2R5.

CTRACE COMP(SYSTCPIS) subcommand

This topic describes the Communications Server CTRACE COMP(SYSTCPIS) subcommand options for z/OS V2R5.

There is no new or changed CTRACE COMP(SYSTCPIS) subcommand option for z/OS V2R5.

CTRACE COMP(SYSTCPOT) subcommand

This topic lists changes to Communications Server CTRACE COMP(SYSTCPOT) subcommand options for z/OS V2R5.

There is no new or changed CTRACE COMP(SYSTCPOT) subcommand option for z/OS V2R5.

CTRACE COMP(SYSTCPRE) subcommand

This topic describes the CTRACE COMP(SYSTCPRE) subcommand options for z/OS V2R5.

There is no new or changed CTRACE COMP(SYSTCPRE) subcommand option for z/OS V2R5.

TCPIPCS subcommand

This topic describes the Communications Server TCPIPCS subcommand option changes for z/OS V2R5.

Table 74 on page 92 lists the TCPIPCS subcommand options.

The TCPIPCS command contains the OPTLOCAL specification in some displays.

Table 74. New and changed Communications Server TCPIPCS subcommand options for z/OS V2R5

Subcommand	Description	Reason for change
CONFIG	The unassociated ISM interfaces will be displayed.	Shared Memory Communications multiple IP subnet support (SMCv2)
MAP POLICY	Includes zERT enforcement policy information in the output.	zERT policy-based enforcement
POLICY	Includes zERT enforcement policy information in the output.	zERT policy-based enforcement
PROFILE	Displays the new INTVAL and SYNCVAL sub-parameters for the GLOBALCONFIG statement.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
PROFILE	The configured values for GLOBALCONFIG POLICYREQUIRED and IKEDREQUIRED will be displayed.	Notification of availability of TCP/IP extended services
PROFILE	The configured SMCEIDs and the SYSTEMEID will be displayed. The configured SMCPERMIT entries and SMCEXCLUDE entries will be displayed. New Interface keywords (SMCRIPADR, PFID, SMCRMTU) are displayed for the OSA interface.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
PROFILE	The display includes the new Sysplex Monitor subparameters – DELAYJOINIPSEC and MONIPSEC.	Sysplex Autonomics for IPSec

Table 74. New and changed Communications Server TCPIPCS subcommand options for z/OS V2R5 (continued)		
Subcommand	**Description**	**Reason for change**
STATE	The report includes a new table, the IKED Heartbeat Historical Data table	Sysplex Autonomics for IPSec
TTLS	The new parameters, ClientExtendedMasterSecret and ServerExtendedMasterSecret, are formatted in a dump of a TCP/IP address space.	AT-TLS currency with System SSL
TTLS	The new parameter ServerKexECurves is displayed for the environment action. It is also displayed for the connection action, if configured.	AT-TLS support for x25519 and x448 key exchange for TLSv1.2
TTLS	The new parameters, GSK_SYSPLEX_SESSION_TICKET_CACHE and GSK_SESSION_TICKET_CLIENT_MAXCACHED, HostReferenceIdDNS, HostReferenceIdCN, and HostRefWildcardValidation are formatted in a dump of a TCP/IP address space.	AT-TLS currency with System SSL

General updates to IPCS subcommands

There are no general updates to IPCS subcommands for z/OS V2R5.

SNMP MIB modules

This topic lists updates to Communications Server's support for SNMP MIB modules.

There are no new or changed SNMP MIB modules for z/OS V2R5.

User exits

For a complete list of supported user exits, refer to *z/OS Communications Server: IP Configuration Reference*.

Table 75 on page 93 lists the updates made to the user exits.

Table 75. New and changed Communications Server user exits for z/OS V2R5		
Exit	**Description**	**Reason for change**
CSSMTP user exit version 3 and version 4	New version 4 CSSMTP user exit. Version 4 is like Version 3 but provides additional information about the job that spooled the SYSOUT including the jobname, the job ID, and the job userid.	PH42487

Application data

There are no new or changed application data for z/OS V2R5.

FTP client error codes

This topic describes new client error codes for the FTP client.

There are no new or changed FTP client error codes for z/OS V2R5.

SMF record type 119 enhancements

See New and changed System Management Facilities (SMF) records for z/OS V2R5 in z/OS Release Upgrade Reference Summary for information on new and changed SMF type 119 records.

See the Type 119 SMF records topic in z/OS Communications Server: IP Programmer's Guide and Reference for more information.

z/OS UNIX /etc files

Changes to z/OS UNIX /etc files are listed in *IP Services: Update /etc configuration files* in z/OS Upgrade Workflow.

General updates of IP interfaces

There are no general updates of IP interface for z/OS V2R5.

Samples provided in MVS data set SEZAINST

Table 76 on page 94 lists the changes to the samples that are provided in MVS data set SEZAINST.

Table 76. IP samples provided in MVS data set SEZAINST for z/OS V2R5

Member	Description	Reason for change
CSSMTPCF	This CSSMTP sample configuration file is updated to add information about ReportMailFrom, ReportSysoutClass, and MailBoxCompatibility.	SMTPD compatibility enhancements for CSSMTP
CSSMTPCF	This CSSMTP sample configuration file is updated to indicate Version4 as a supported UserExit value.	PH42487
EZARACF	The sample RACF commands are updated to provide commands for using the RDATALIB class to protect keyring access.	Release updates
EZARACF	A new resource profile in the SERVAUTH class is provided for the EZB.FTP.*sysname.ftpdaemonname*.ACCESS.JES resource	FTP server JES access control
EZAFTPAS	Sample FTP.DATA file for the FTP server. Removed CIPHERSUITE, KEYRING, SSLV3, and TLSTIMEOUT statements.	Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
SYSLOGD	The syslog daemon started procedure sample is updated to use a REGION=0M.	z/OS UNIX syslogd support for secure logging over TCP

Samples provided in z/OS UNIX TCPIP directory

Table 77 on page 94 lists the changes to the samples that are provided in z/OS UNIX directory /usr/lpp/tcpip/samples.

Table 77. IP samples provided in z/OS UNIX directory /usr/lpp/tcpip/samples for z/OS V2R5

File name	Description	Reason for change
iked.conf	The IKE configuration file sample has been updated to add the NoKeyRing parameter.	Sysplex Autonomics for IPSec

Table 77. IP samples provided in z/OS UNIX directory /usr/lpp/tcpip/samples for z/OS V2R5 (continued)		
File name	**Description**	**Reason for change**
pagent.conf	The main pagent configuration file has been updated to add zERT enforcement policy information.	zERT policy-based enforcement
pagent_ZERT.conf	A new sample file with zERT enforcement policy definitions.	zERT policy-based enforcement
syslog.conf	The syslog daemon configuration file sample has been updated to add the new -A forwarding action.	z/OS UNIX syslogd support for secure logging over TCP

Communications Server SNA interface changes

This topic describes the following Communications Server SNA interfaces:

Start options

Table 78 on page 95 lists the new or changed SNA start options.

Refer to *z/OS Communications Server: SNA Resource Definition Reference* for more information on start options.

Table 78. New and changed Communications Server start options for z/OS V2R5		
Start option	**Description of update**	**Reason for change**
• OSIEVENT • OSIMGMT • OSITOPO • UPDDELAY	These start options are deleted.	Removal of CMIP from VTAM
QDIOEIB	When set to ENABLED, specifies that VTAM will enable the Enhanced Inbound Blocking (EIB) function within the OSA-Express feature for all eligible QDIO interfaces for all TCP/IP stacks.	OSA-Express Enhanced Inbound Blocking (EIB)

Start option behavior changes

There are no start option behavior changes for z/OS V2R5.

Definition statements

Table 79 on page 96 lists the changes to SNA definition statements.

For complete information about all changed and new definition statements, see *z/OS Communications Server: SNA Resource Definition Reference*.

Table 79. New and changed Communications Server definition statements for z/OS V2R5		
Definition statement	**Description of update**	**Reason for change**
VTAMTOPO	The statement is removed from all SNA resources (Group, LINE, PORT, PU, etc).	Removal of CMIP from VTAM

Commands

Table 80 on page 96 lists the new and changed SNA commands.

For complete information about SNA commands, refer to the *z/OS Communications Server: SNA Operation*.

Table 80. New and changed Communications Server commands in z/OS V2R5		
Command	**Description**	**Reason for change**
Modify VTAMOPTS	Modify command is rejected for OSIMGMT, OSITOPO, OSIEVENT and UPDDELAY start options.	Removal of CMIP from VTAM
Modify resource, VTAMTOPO	VTAMTOPO resource definition is being deleted.	
Modify TRACE,TYPE,BUF or IO	CMIP trace options is removed.	

Command behavior changes

Table 81 on page 96 lists the SNA commands that have changed behavior.

For complete information about SNA commands, refer to the *z/OS Communications Server: SNA Operation*.

Table 81. New and changed Communications Server commands with changed behavior for z/OS V2R5		
Command	**Description of behavior change**	**Reason for change**
D NET,ID=*trle*	A TRLE for an unassociated ISM device will display **NA** for the PNETID.	Shared Memory Communications multiple IP subnet support (SMCv2)
D NET,TRL,TRLE=	• A TRLE for an unassociated ISM device will display **NA** for the PNETID. • When DEVSTATS is specified for a RNIC TRLE, statistics for ethernet frames related to ARP processing will be displayed.	Shared Memory Communications multiple IP subnet support (SMCv2)
DISPLAY ID	• If the resource that is being displayed is a RDMA over Converged Ethernet (RoCE) TRLE, message IST2389I contains the "RoCE Express" generation level and the transmission speed. RoCE Express3 was added to the RoCE Express generation level. • If the resource that is being displayed is a RoCE Express3 TRLE, message IST2362I always displays the microcode level.	Communications Server support for RoCE Express3

Table 81. New and changed Communications Server commands with changed behavior for z/OS V2R5 (continued)		
Command	**Description of behavior change**	**Reason for change**
DISPLAY TRL	• If the TRLE operand specifies a RDMA over Converged Ethernet (RoCE) TRLE, message IST2389I contains the "RoCE Express" generation level and the transmission speed. RoCE Express3 was added to the RoCE Express generation level. • If the TRLE operand specifies a RoCE Express3 TRLE, message IST2362I always displays the microcode level.	Communications Server support for RoCE Express3

VTAM CMIP Services

Table 82 on page 97 lists the SNA VTAM CMIP services that have changed behavior.

Table 82. New and changed VTAM CMIP services with changed behavior for z/OS V2R5		
CMIP services	**Description of behavior change**	**Reason for change**
Deprecated	CMIP services and TOPO agent are deprecated	Removal of CMIP from VTAM

VTAM internal trace entries

For complete information about VIT entries, see *z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT*.

Table 83 on page 97 lists the new and changed VIT entries.

Table 83. New and changed Communications Server VTAM internal trace (VIT) entries for z/OS V2R5		
VIT entry	**Description**	**Reason for change**
CMER, CME2, MCO1, MCO2, MDEL, MDIS, MQRQ, MQRS, MREG, MRG, MRG2, RQE	**Deleted:** These entries are being deleted.	Removal of CMIP from VTAM
ENFx	Updated to record the driving of an ENF exit for an ISM device.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)
RPLA	A count field was added to the RPLA VIT entry.	Shared Memory Communications multiple IP subnet support (SMCv2: SMC-Rv2 and SMC-Dv2)

VTAMMAP Formatted Dump changes

There are no VTAMMAP formatted dump changes for z/OS V2R5.

Tuning statistics reports

This topic lists the Communications Server SNA tuning statistics reports changes for z/OS V2R5.

There are no new and changed tuning statistics reports for z/OS V2R5.

Chapter 5. V2R4 new function summary

This information contains topics about every function or enhancement introduced in z/OS V2R4 Communications Server. The topics describe each function and present the following information, if applicable:

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

See Chapter 2, "Roadmap to functions," on page 19 for a complete list of the functional enhancements.

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

See z/OS Release Upgrade Reference Summary for information about new and changed messages and interfaces.

Simplification

The following topics describe enhancements for simplification:

- "Communications Server exploitation of the IBM Function Registry for z/OS" on page 99
- "IBM Health Checker for the removal of VTAM LSA Architecture" on page 99
- "IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity" on page 100

Communications Server exploitation of the IBM Function Registry for z/OS

z/OS V2R4 Communications Server, with SNA APAR OA63555, is enhanced to register VTAM general information with the IBM Function Registry for z/OS. This information allows you to understand the extent of SNA application activity in your network.

Using Communications Server exploitation of the IBM Function Registry for z/OS

To use Communications Server exploitation of the IBM Function Registry for z/OS, complete the appropriate tasks in Table 84 on page 99.

Table 84. Task topics to enable Communications Server exploitation of the IBM Function Registry for z/OS

Task	Reference
Use the IBM FXEPRINT utility function Issue the DISPLAY FXE command	VTAM usage of IBM Function Registry for z/OS in z/OS Communications Server: SNA Network Implementation Guide

IBM Health Checker for the removal of VTAM LSA Architecture

z/OS V2R4 Communications Server, with SNA APAR OA62208, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies if VTAM Link Station Architecture (LSA) devices are in use. These devices are configured with MEDIUM=CSMACD in the XCA major node PORT statement.

Support for VTAM Link Station Architecture (LSA) devices will be withdrawn in a future release of the IBM z/OS Communications Server.

Dependency:

To use the IBM Health Checker for the removal of VTAM LSA Architecture, perform the following steps:

- Apply the appropriate PTF for SNA APAR OA62208
- Start the IBM Health Checker for z/OS

Using the IBM Health Checker for the removal of VTAM LSA Architecture

To use the IBM Health Checker for the removal of VTAM LSA Architecture, perform the tasks in Table 85 on page 100.

Table 85. IBM Health Checker for the removal of VTAM LSA Architecture

Task/Procedure	Reference
To use this migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R5_NEXT_CS_LSA migration health check. 3. Review health check output messages ISTM051I or ISTM052E for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for the removal of VTAM LSA Architecture, see Table 86 on page 100.

Table 86. All related topics about IBM Health Checker for the removal of VTAM LSA Architecture

Book name	Topics
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R5_NEXT_CS_LSA
z/OS Upgrade Workflow	*SNA and IP services: Prepare for the removal of support for LSA and LCS devices*
z/OS Communications Server: SNA Messages	• ISTM051I • ISTM052E

IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity

z/OS V2R4 Communications Server, with SNA APAR OA62208 and TCP/IP APAR PH40875, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies if TCP/IP profile statements DEVICE, LINK, and HOME for OSA-Express connectivity are in use.

Support for DEVICE/LINK/HOME TCP/IP profile statements for OSA-Express connectivity will be withdrawn in a future release of IBM z/OS Communications Server.

Dependency:

To use the IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity, perform the following steps:

- Apply the appropriate PTF for SNA APAR OA62208
- Apply the appropriate PTF for TCP/IP APAR PH40875
- Start the IBM Health Checker for z/OS

Using the IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity

To use the IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity, perform the tasks in Table 87 on page 101.

Table 87. IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity

Task/Procedure	Reference
To use this migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R5_NEXT_CS_OSADLH migration health check. 3. Review health check output messages ISTM053I or ISTM054E for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity, see Table 88 on page 101.

Table 88. All related topics about IBM Health Checker for the removal of DEVICE, LINK, and HOME for OSA-Express connectivity

Book name	Topics
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R5_NEXT_CS_OSADLH
z/OS Upgrade Workflow	*IP Services: Prepare for the removal of support for OSA DEVICE/LINK/HOME configuration*
z/OS Communications Server: SNA Messages	• ISTM053I • ISTM054E

Hardware support

The following topics describe enhancements for hardware support:

OSA-Express Enhanced Inbound Blocking (EIB)

In z/OS V2R4 Communications Server, with TCP/IP APAR PH44281 and SNA APAR OA62831, OSA-Express Enhanced Inbound Blocking (EIB) is a QDIO performance enhancement that might be beneficial for OSA interfaces with a high volume of inbound network bulk or streaming traffic.

Restriction:

QDIO Enhanced Inbound Blocking is supported on OSA-Express7s on z16 or later systems (with supporting MCL) and subsequent systems only.

Using OSA-Express Enhanced Inbound Blocking (EIB)

To use OSA-Express Enhanced Inbound Blocking (EIB), perform the tasks in Table 89 on page 102.

Table 89. Task topics to enable OSA-Express Enhanced Inbound Blocking (EIB)

Task/Procedure	Reference
• Configure VTAM start option QDIOEIB to enable OSA-Express Enhanced Inbound Blocking. • Verify that the QDIOEIB start option is enabled.	• QDIOEIB start option in z/OS Communications Server: SNA Resource Definition Reference • DISPLAY VTAMOPTS command in z/OS Communications Server: SNA Operation
• Verify that the QDIOSTG start option is set to: – MAX or 126 for 25 gigabit OSA features. – 126 for gigabit or 10 gigabit OSA features.	• Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
• Verify that INBPERF DYNAMIC (with or without WORKLOADQ) is set on eligible OSA interfaces via Netstat DEvlinks.	• Interface statement in z/OS Communications Server: IP Configuration Reference
Display whether OSA-Express Enhanced Inbound Blocking is enabled by issuing the DISPLAY TCPIP,,OSAINFO command.	• DISPLAY TCPIP,,OSAINFO in z/OS Communications Server: IP System Administrator's Commands

To find all new and updated topics about OSA-Express Enhanced Inbound Blocking (EIB), see Table 90 on page 102.

Table 90. All related topics about OSA-Express Enhanced Inbound Blocking (EIB)

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Fixed storage considerations for OSA-Express interfaces in QDIO mode
z/OS Communications Server: IP Configuration Reference	• Interface statement • DEVICE and LINK - MPCIPA OSA-Express QDIO devices statement • INTERFACE-IPAQENET OSA-Express QDIO interfaces • INTERFACE-IPAQENET6 OSA-Express QDIO interfaces
z/OS Communications Server: IP System Administrator's Commands	• DISPLAY TCPIP,,OSAINFO • Netstat DEvlinks/-d report
z/OS Communications Server: SNA Operation	• DISPLAY VTAMOPTS command • MODIFY VTAMOPTS command • START command
z/OS Communications Server: SNA Resource Definition Reference	• QDIOEIB start option • Start options syntax diagrams • QDIOSTG start option

Table 90. All related topics about OSA-Express Enhanced Inbound Blocking (EIB) (continued)	
Book name	**Topics**
z/OS Communications Server: Quick Reference	• F VTAMOPTS command • Start options

Communications Server support for RoCE Express3

z/OS V2R4 Communications Server, with TCP/IP APAR PH34117 and SNA APAR OA60855, extends the Shared Memory Communications over Remote Direct Memory Access (SMC-R) function to support the next generation IBM RoCE Express3 feature. The IBM RoCE Express3 feature allows TCP/IP stacks on different LPARs within the same central processor complex (CPC) to leverage the power of these state-of-the-art adapters to optimize network connectivity for mission critical workloads by using Shared Memory Communications technology.

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

Dependencies: This function requires the IBM z16 or later systems. To enable the z/OS Communications Server support for RoCE Express3 features, complete the appropriate tasks in the following table.

Using Communications Server support for RoCE Express3

To use Communications Server support for RoCE Express3, complete the appropriate tasks in Table 91 on page 103.

Table 91. Task topics to enable Communications Server support for RoCE Express3	
Task	**Reference**
Configure at least one IBM RoCE Express3 feature in HCD. For each RoCE Express3 port, configure the physical network ID (PNetID), the physical channel ID (PCHID), the Function ID (FID), the virtual function ID (VF), and the port number (PORTNUM).	z/OS HCD User's Guide
Configure or update the GLOBALCONFIG SMCR statement in the TCP/IP profile. • Use the FID values configured in HCD to define the PFID values that represent physically different RoCE Express3 features to provide full redundancy support. • Do not specify PortNum for RoCE Express3 PFIDs, or specify the PORTNUM value configured in HCD for the PFID.	• GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference • Shared Memory Communications over Remote Direct Memory Access in z/OS Communications Server: IP Configuration Guide
Display information about a RoCE Express3 interface by issuing the Netstat DEvlinks/-d command and specifying the name of the RoCE Express3 interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about Communications Server support for RoCE Express3, see Table 92 on page 104.

Table 92. All related topics about Communications Server support for RoCE Express3

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• RoCE Express3 feature environment • Connectivity and gateway functions • Shared Memory Communications terms • VLANID considerations • Physical network considerations • System requirements for SMC-R in a shared RoCE environment • System requirements for SMC-D • Configuring Shared Memory Communications over RDMA • VTAM displays and tuning statistics
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP/IP profile record Global configuration section • RDMA network interface card (RNIC) interface statistics record (subtype 44)
z/OS Communications Server: IP System Administrator's Commands	• Netstat CONFIG/-f report • Netstat DEvlinks/-d report
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command • MODIFY CSDUMP command
z/OS Communications Server: SNA Network Implementation Guide	• Resources automatically activated by VTAM
z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	• HCQ entry for invoking a RoCE HCQ operation (Part 1) • HCQ2 entry for invoking a RoCE HCQ operation (Part 2) • HCQ3 entry for invoking a RoCE HCQ operation (Part 3) • HCQ4 entry for invoking a RoCE HCQ operation (Part 4) • HCQ5 entry for invoking a RoCE HCQ operation (Part 5) • HCQ6 entry for invoking a RoCE HCQ operation (Part 6)
z/OS Communications Server: SNA Resource Definition Reference	• CSDUMP start option
z/OS Communications Server: IP and SNA Codes	• Data link control (DLC) status codes
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ4336I

Table 92. All related topics about Communications Server support for RoCE Express3 (continued)	
Book name	**Topics**
z/OS Communications Server: SNA Messages	• IST2361I • IST2396I • IST2444I
z/OS HCD User's Guide	N/A

Shared Memory Communications multiple IP subnet support (SMCv2)

In z/OS V2R4 Communications Server, with TCP/IP APAR PH22695 and SNA APAR OA59152, Shared Memory Communications - Direct Memory Access (SMC-D) is enhanced to remove the same subnet restriction by exploiting SMC-Dv2.

Dependencies:

- SMC-Dv2 is enabled with new IBM Z capability provided by the IBM Z Internal Shared Memory (ISM) function. The new ISMv2 capability is available on IBM z15 or later systems. For IBM z15 T01, refer to the MCL number P46601.067 driver D41C. The ISMv2 support is in the base of the IBM z15 T02.

Downlevel SMC partners might require a toleration PTF. If you plan to enable SMC-Dv2 on a host which has connections to a down-level SMC (SMC-Dv1 or SMC-Rv1) system (z/OS Communications Server, Linux on Z, and AIX), the down-level host will require the following toleration maintenance applied prior to enabling SMC-Dv2:

- For z/OS Communications Server, the down-level host will need the appropriate PTF for PH17556.
- For Linux on Z, see the Linux on Z web page at https://linux-on-z.blogspot.com/p/smc-for-linux-on-ibm-z.html for information related to toleration requirements.
- For AIX, see the AIX web page at https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/rdma/smc_r.html for information related to toleration requirements.

Note: Failure to apply the proper toleration maintenance might result in connection hangs or failures when SMC-Dv2 is enabled on z/OS.

The PTF for z/OS IOS PCIe Services APAR OA59235 is required. Failure to apply that PTF will result in activation failures.

Using the Shared Memory Communications multiple IP subnet support (SMCv2)

To use the Shared Memory Communications multiple IP subnet support (SMCv2), perform the tasks in Table 93 on page 105.

Table 93. Shared Memory Communications multiple IP subnet support (SMCv2)	
Task/Procedure	**Reference**
Determine if using SMC will be a benefit in this configuration by using SMCAT.	VARY TCPIP,,SMCAT about SMC Applicability Tool (SMCAT) in z/OS Communications Server: IP System Administrator's Commands
Configure SMCEID on the SMCGLOBAL parameter of the GLOBALCONFIG statement to enable z/OS CS exploitation of SMC-Dv2.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Configure SYSTEMEID on the SMCD parameter of the GLOBALCONFIG statement to enable z/OS CS exploitation of SMC-Dv2.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference

Table 93. Shared Memory Communications multiple IP subnet support (SMCv2) (continued)	
Task/Procedure	**Reference**
Display whether SMCEID values were specified on SMCGLOBAL by issuing the Netstat CONFIG/-f command.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display SMC version used for a connection or link.	z/OS Communications Server: IP System Administrator's Commands: • Netstat ALL/-A report • Netstat DEvlinks/-d report
Display all interfaces z/OS CS used for SMC communications.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display information about the dynamic ISM TRLEs by issuing the D NET,ID=*trle*, or D NET,TRL,TRLE=*trle* command, which might now show **NA** for the PNETID.	z/OS Communications Server: SNA Operation • DISPLAY ID command • DISPLAY TRL command

To find all new and updated topics about Shared Memory Communications multiple IP subnet support (SMCv2), see .

Table 94. All related topics about Shared Memory Communications multiple IP subnet support (SMCv2)	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Shared Memory Communications multiple IP subnet support (SMCv2) • Physical network considerations • VLANID considerations • Configuring Shared Memory Communications - Direct Memory Access
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP connection termination record (subtype 2) • SMC-D link statistics record (subtype 38) • SMC-D link state start record (subtype 39) • SMC-D link state end record (subtype 40) • TCP/IP profile record Global configuration section
z/OS Communications Server: IP Diagnosis Guide	• Diagnosing problems with Shared Memory Communications • Physical network ID configuration issues • No associated subnet mask
z/OS Communications Server: IP System Administrator's Commands	• DISPLAY TCPIP,,NETSTAT • VARY TCPIP,,SMCAT • Netstat ALL/-A report • Netstat CONFIG/-f report • Netstat DEvlinks/-d report

Table 94. All related topics about Shared Memory Communications multiple IP subnet support (SMCv2) (continued)	
Book name	**Topics**
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command
z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	• ENFx entry for ENF exit • RPLA entry for invoking a RoCE Poll command (Part 3)
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD2051I
z/OS Communications Server: SNA Messages	• IST2418I • IST2421I • IST2464I • IST2465I

Communications Server support for OSA-Express7S 25 GbE features

z/OS V2R4 Communications Server is enhanced to support the OSA-Express7S feature with 25 GbE bandwidth.

Using Communications Server support for OSA-Express7S 25 GbE features

To enable Communications Server support for OSA-Express7S 25 GbE features, complete the appropriate tasks in Table 95 on page 107.

Table 95. Task topics to enable Communications Server support for OSA-Express7S 25 GbE features	
Task	**Reference**
Display the generation level and speed for an active OSA-Express7S QDIO interface by issuing the **DISPLAY TCPIP,,OSAINFO** command.	DISPLAY TCPIP,,OSAINFO in z/OS Communications Server: IP System Administrator's Commands
Display the interface speed value for an active OSA-Express7S QDIO interface by issuing the **Netstat DEvlinks/-d** command.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display the read storage value for an active OSA-Express7S QDIO interface by issuing the **Netstat DEvlinks/-d** command.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display the read storage value for an active OSA-Express7S QDIO data device by issuing the **D TRL,TRLE=***trle* command.	DISPLAY TRL command in z/OS Communications Server: SNA Operation
Determine the amount of fixed storage that will be allocated for each OSA-Express QDIO interface.	Fixed storage considerations for OSA-Express interfaces in QDIO mode in z/OS Communications Server: IP Configuration Guide
Consider whether to increase the FIXED MAX setting in your IVTPRM00 parmlib member.	Fixed maximum storage for CSM buffers in z/OS Communications Server: IP Configuration Guide

To find all related topics about Communications Server support for OSA-Express7S 25 GbE features, see Table 96 on page 108.

Table 96. All related topics about Communications Server support for OSA-Express7S 25 GbE features	
Book name	**Topics**
IP Configuration Guide	• Fixed storage considerations for OSA-Express interfaces in QDIO mode • Fixed maximum storage for CSM buffers • Additional fixed storage for OSA interfaces using 8 MB of read storage
IP Configuration Reference	• INTERFACE-IPAQENET OSA-Express QDIO interfaces • INTERFACE-IPAQENET6 OSA-Express QDIO interfaces • DEVICE and LINK - MPCIPA OSA-Express QDIO devices statement
IP System Administrator's Commands	• DISPLAY TCPIP,,OSAINFO • Netstat DEvlinks/-d report • Reply field descriptions
SNA Operations	• DISPLAY TRL command • DISPLAY VTAMOPTS command • START command
SNA Resource Definition Reference	• QDIOSTG start option

Communications Server support for 25 GbE RoCE Express2 features

z/OS Communications Server V2R4 is enhanced to support IBM 25 GbE RoCE Express2 features.

Using Communications Server support for 25 GbE RoCE Express2 features

To enable the z/OS Communications Server support for 25 GbE RoCE Express2 features, complete the appropriate tasks in Table 97 on page 108.

Table 97. Task topics to enable z/OS Communications Server support for 25 GbE RoCE Express2 features	
Task	**Reference**
Configure at least one IBM 25 GbE RoCE Express2 feature in HCD. For each IBM RoCE Express2 port, configure the physical network identifier (PNetID), the physical channel identifier (PCHID), the function identifier (FID), the virtual function identifier (VF), and the port number (PORTNUM).	z/OS HCD User's Guide
Configure or update the GLOBALCONFIG SMCR statement in the TCP/IP profile. • Use the FID values configured in HCD to define the PFID values that represent physically different IBM 25 GbE RoCE Express2 features to provide full redundancy support. Do not specify PortNum for IBM RoCE Express2 PFIDs.	• GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference • Shared Memory Communications over Remote Direct Memory Access in z/OS Communications Server: IP Configuration Guide

Table 97. Task topics to enable z/OS Communications Server support for 25 GbE RoCE Express2 features (continued)	
Task	**Reference**
Display information about a RoCE Express2 interface, including the interface speed, by issuing the Netstat DEvlinks/-d command and specifying the RoCE Express2 interface name.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about Communications Server support for 25 GbE RoCE Express2 features, see Table 98 on page 109.

Table 98. All related topics about z/OS Communications Server support for 25 GbE RoCE Express2 features	
Book name	**Topics**
IP Configuration Guide	• Shared Memory Communications terms • SMC-R link groups • System requirements for SMC-R in a shared RoCE environment
IP Configuration Reference	• GLOBALCONFIG statement
IP System Administrator's Commands	• Netstat DEvlinks/-d report
SNA Messages	• IST2361I
z/OS HCD User's Guide	N/A

Communications Server QDIO display enhancements

Starting with z/OS Communications Server V2R4, read errors, if any, on the OSA inbound queues are displayed under the queue ID when VTAM TRLE display commands are issued.

Using Communications Server QDIO display enhancements

To enable Communications Server QDIO display enhancements, complete the appropriate tasks in Table 99 on page 109.

Table 99. Task topics to enable Communications Server QDIO display enhancements	
Task/Procedure	**Reference**
To see information about OSA read errors on the inbound queues, issue the command D NET,ID=*trle_name* or D NET,TRL,TRLE=*trle_name*. If there are OSA read errors, they will be displayed under the queue ID.	• DISPLAY ID command in z/OS Communications Server: SNA Operation • DISPLAY TRL command in z/OS Communications Server: SNA Operation

To find all related topics about Communications Server QDIO display enhancements, see Table 100 on page 109.

Table 100. All related topics about Communications Server QDIO display enhancements	
Book name	**Topics**
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command

Table 100. All related topics about Communications Server QDIO display enhancements (continued)	
Book name	**Topics**
z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	• ODPK entry for OSA-Express QDIO or HiperSockets packets (Part 1)
z/OS Communications Server: SNA Messages	• IST1221I • IST2457I • IST2458I • IST2459I • IST2460I • IST2461I • IST2462I • IST2463I

Usability and skills

The following topics describe enhancements for usability and skills:

- "HiperSockets Converged Interface support" on page 110

HiperSockets Converged Interface support

z/OS V2R4 Communications Server provides HiperSockets Converged Interface (HSCI) solution to support the z/VM bridge environment. With this solution, a Linux guest can connect to z/OS via Layer 2 HiperSockets and to the external network by using a single IP interface.

This support also significantly improves HiperSockets usability by dynamically provisioning and activating a HiperSockets interface when an OSD interface is activated for the same physical network ID (PNetID). With this support, the TCP/IP stack only sees the OSD interface. This design approach greatly reduces the network administration costs as HiperSockets interfaces no longer are required to be configured, operated, or managed in z/OS Communications Server. This solution allows a single IP interface (OSD) to provide access to the external Ethernet LAN and transparent access to HiperSockets for LPAR to LPAR communications within the central processor complex (CPC). This solution also eliminates the need to reconfigure z/OS HiperSockets interfaces when moving a z/OS instance from one CPC to another. The HSCI is also referred to as an IQDC interface.

Incompatibilities:

- This function does not support IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.
- This function also requires the virtual MAC (VMAC) operand be specified on your IPAQENET interfaces to request OSA-generated VMACs.

Dependencies:

- This function minimally requires a zEnterprise EC12 (zEC12).
- This function requires an Internal Queued Direct I/O (IQD) channel path ID (CHPID) configured with the external bridge function.

Using HiperSockets Converged Interface support

To enable HiperSockets Converged Interface support, perform the tasks in Table 101 on page 111.

Table 101. HiperSockets Converged Interface support	
Task/Procedure	**Reference**
If you use IPv4 Queued Direct I/O (QDIO) interfaces that are defined with the DEVICE, LINK, and HOME statements, convert those definitions to use the IPAQENET INTERFACE statement.	Steps for converting from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement in z/OS Communications Server: IP Configuration Guide
Configure at least one IQD CHPID with the external bridge function in hardware configuration definition (HCD). For each bridged IQD CHPID, configure at least 10 channel unit addresses (CUAs) for each protocol (IPv4 and IPv6) that your network supports. If you use jumbo frames for your OSD interfaces that are associated with a converged HiperSockets CHPID, specify an IQD frame size larger than 16 K when you configure your converged HiperSockets CHPID. This avoids fragmentation, which allows more traffic to flow over the converged HiperSockets interface.	z/OS HCD User's Guide
Select a unique physical network ID (PNetID) for each of your networks. Configure the appropriate PNetID in HCD for each OSD CHPID on a network and configure the same PNetID on each bridged IQD CHPID to be used on that network. If you already have a PNetID configured on your OSD CHPID for Shared Memory Communications, configure the same PNetID on your bridged IQD CHPID.	z/OS HCD User's Guide
Configure AUTOIQDC on the GLOBALCONFIG statement in the TCP/IP profile.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display whether the stack is enabled for dynamic IQDC interfaces and whether large outbound TCP socket sends should use these interfaces.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Display information about the dynamic IQDC TRLEs and datapath devices by issuing the **D NET,ID=trle**, or **D NET,TRL,TRLE=** command.	z/OS Communications Server: SNA Operation • DISPLAY ID command • DISPLAY TRL command
Display the dynamically generated name of an IQDC interface by issuing the **Netstat DEvlinks/-d** command against the associated OSD interface. Extract the name from the "Associated IQD Converged Interface" output line.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display information about the number of packets and bytes which went over the dynamic IQDC interface by issuing the **Netstat DEvlinks/-d** command against the IQDC interface.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display the ARP cache entries that are associated with an IPv4 IQDC interface by issuing the **Netstat ARp/-R** command.	Netstat ARp/-R report in z/OS Communications Server: IP System Administrator's Commands
Display the neighbor cache entries that are associated with an IPv6 IQDC interface by issuing the **Netstat ND/-n** command.	Netstat ND/-n report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about HiperSockets Converged Interface support, see Table 102 on page 112.

Table 102. All related topics about HiperSockets Converged Interface support

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• z/OS HiperSockets Layer 3 connectivity – HiperSockets Converged Interface overview – Linux and z/VM VSwitch bridge considerations – Performance considerations for HiperSockets Converged Interface – SMC and HSCI PNetID considerations – Steps for enabling HiperSockets Converged Interface – Steps for converting from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement
z/OS Communications Server: IP Diagnosis Guide	• OPTIONS syntax • OPTIONS keywords
z/OS Communications Server: IP Programmer's Guide and Reference	• Common real-time trace record attributes • TCP/IP profile record Global configuration section • Interface statistics record (subtype 6)
z/OS Communications Server: IP System Administrator's Commands	• Netstat ARp/-R report • Netstat: CONFIG/-f report • Netstat DEvlinks/-d report • Netstat ND/-n report
z/OS Communications Server: IP and SNA Codes	• Data link control (DLC) status codes
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command
z/OS Communications Server: SNA Network Implementation Guide	• Resources automatically activated by VTAM
z/OS Communications Server: SNA Resource Definition Reference	• Operation-level USS table (ISTINCNO)
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD2028I
z/OS Communications Server: SNA Messages	• IST1016I • IST1221I • IST2319I

Scalability and performance

The following topics describe enhancements for scalability and performance:

zERT Aggregation recording interval

z/OS V2R4 Communications Server with APAR PH25049 provides a zERT Aggregation recording interval that is not bound to the system SMF interval. This interval allows zERT summary records to be generated at an interval that can range from 1 to 24 hours.

Note: With APAR PH24543, you can configure this function in the Network Configuration Assistant (NCA).

zERT summary records can be collected as SMF type 119, subtype 12 records in the System Management Facility data sets or log streams. zERT summary records can also be collected by a real-time NMI application using the SYSTCPES service.

Warning:

Decreasing the frequency at which zERT summary records are written can increase the amount of 64-bit pageable, private memory needed. This is because zERT aggregation information is held longer in memory before being captured in SMF records.

Using the zERT Aggregation recording interval

To use the zERT Aggregation recording interval, perform the tasks in Table 103 on page 113.

Table 103. zERT Aggregation recording interval

Task/Procedure	Reference
Determine if you want to use the zERT aggregation recording interval.	Enabling a longer zERT aggregation recording interval in z/OS Communications Server: IP Configuration Guide
Enable the zERT aggregation recording interval using the new INTVAL and SYNCVAL sub-parameters on the GLOBALCONFIG ZERT AGGREGATION statement.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display zERT aggregation recording interval settings.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands

To find all new and updated topics about zERT Aggregation recording interval, see Table 104 on page 113.

Table 104. All related topics about zERT Aggregation recording interval

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Enabling a longer zERT aggregation recording interval • z/OS Encryption Readiness Technology (zERT) Concepts • How does zERT aggregation provide the information? • Enabling zERT aggregation • Setting up TCP/IP operating characteristics in PROFILE.TCPIP

Table 104. All related topics about zERT Aggregation recording interval (continued)	
Book name	**Topics**
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement
z/OS Communications Server: IP System Administrator's Commands	• D TCPIP,,STOR command • Netstat CONFIG/-f report
z/OS Communications Server: IP Programmer's Guide and Reference	• Format and details for poll-type requests • TCP/IP statistics record (subtype 5) • zERT Summary record (subtype 12) • TCP/IP profile record Global configuration section
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ8455I

Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions

z/OS V2R4 Communications Server, with VTAM APAR OA58300 and TCP/IP APAR PH16581, is enhanced to support inbound workload queueing for IBM z/OS Container Extensions (zCX) workloads for OSA-Express in QDIO mode.

Inbound workload queueing uses multiple input queues for each QDIO data device (subchannel device) to improve TCP/IP stack scalability and general network optimization. To implement the performance improvements for zCX workloads, enable inbound workload queueing to process zCX, IPSec, EE, sysplex distributor, and streaming bulk data traffic all concurrently with other types of inbound QDIO traffic. When you enable these improvements for a QDIO interface, zCX, inbound IPSec, EE, sysplex distributor, and streaming bulk data traffic are each processed on their own ancillary input queue (AIQ). All other inbound traffic is processed on the primary input queue.

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

Dependencies:

- This function is limited to OSA-Express6S Ethernet features or later in QDIO mode running on IBM z14. For more information about the QDIO inbound workload queueing function and the OSA-Express features that support it, see QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide. See the 3906DEVICE or 3907DEVICE Preventive Service Planning (PSP) bucket for more information.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

Using Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions

To enable IWQ support for z/OS Container Extensions, complete the appropriate tasks in Table 105 on page 115.

Table 105. Task topics to enable IWQ support for z/OS Container Extensions	
Task	**Reference**
Enable inbound workload queueing for a specific QDIO interface by specifying the WORKLOADQ parameter on the IPAQENET or IPAQENET6 INTERFACE statement (if not already configured).	• See the following statements in z/OS Communications Server: IP Configuration Reference: – INTERFACE-IPAQENET OSA-Express QDIO interfaces – INTERFACE-IPAQENET6 OSA-Express QDIO interfaces • Steps for enabling QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide
Display whether inbound workload queueing is in effect for the QDIO interface by issuing the **`Netstat DEvlinks/-d`** command.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display whether inbound workload queueing is in effect for the QDIO interface and display the workload queueing functions and queue IDs for that interface by issuing the **`DISPLAY NET,ID=trle`** command or the **`DISPLAY NET,TRL,TRLE=trle`** command.	See the following topics in z/OS Communications Server: SNA Operation: • DISPLAY ID command • DISPLAY TRL command
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by initiating VTAM tuning statistics for the QDIO interface.	MODIFY TNSTAT command in z/OS Communications Server: SNA Operation
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by using the TCP/IP callable NMI GetIfStatsExtended request.	TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer's Guide and Reference
Determine the QID on which a specific packet was received, and the associated workload queueing function, from a packet trace.	Formatting packet traces using IPCS in z/OS Communications Server: IP Diagnosis Guide
Determine the QID on which a specific packet was received from an OSAENTA trace.	Formatting OSA traces using IPCS in z/OS Communications Server: IP Diagnosis Guide

To find all related topics about IWQ support for z/OS Container Extensions, see Table 106 on page 115.

Table 106. All related topics about IWQ support for z/OS Container Extensions	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• QDIO inbound workload queueing
z/OS Communications Server: IP Configuration Reference	• INTERFACE-IPAQENET OSA-Express QDIO interfaces • INTERFACE-IPAQENET6 OSA-Express QDIO interfaces
z/OS Communications Server: IP Programmer's Guide and Reference	• TCP/IP callable NMI (EZBNMIFR)
z/OS Communications Server: IP Diagnosis Guide	• Formatting packet traces using IPCS • Formatting OSA traces using IPCS

Table 106. All related topics about IWQ support for z/OS Container Extensions (continued)	
Book name	**Topics**
z/OS Communications Server: IP System Administrator's Commands	• DISPLAY TCPIP,,OSAINFO • Netstat DEvlinks/-d report
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command • MODIFY TNSTAT command
z/OS Communications Server: SNA Messages	• IST1221I • IST1230I • IST1233I

Sysplex notification of TCP/IP stack join or leave

z/OS V2R4 has enhanced Event Notification Facility code 80 to send a signal when a stack joins or leaves a sysplex group.

Using Sysplex notification of TCP/IP stack join or leave

To enable sysplex notification of TCP/IP stack join or leave, complete the appropriate tasks in Table 107 on page 116.

Table 107. Task topics to enable sysplex notification of TCP/IP stack join or leave	
Task	**Reference**
Create an ENF 80 exit in order to listen for the new signal when a TCP/IP stack joins or leaves a sysplex group.	• EZAENF80 Parameter list for ENF event code 80 listen exits in z/OS Communications Server: IP Programmer's Guide and Reference • Using ENF event code 80 to notify applications of TCP/IP joining or leaving a sysplex in z/OS Communications Server: IP Programmer's Guide and Reference • Listening for system events in z/OS MVS Programming: Authorized Assembler Services Guide • *Table: ENF macro event codes* in z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG

To find all related topics about sysplex notification of TCP/IP stack join or leave, see Table 108 on page 116.

Table 108. All related topics about sysplex notification of TCP/IP stack join or leave	
Book name	**Topics**
z/OS Communications Server: IP Programmer's Guide and Reference	• EZAENF80 Parameter list for ENF event code 80 listen exits • Using ENF event code 80 to notify applications of TCP/IP joining or leaving a sysplex

Table 108. All related topics about sysplex notification of TCP/IP stack join or leave (continued)	
Book name	**Topics**
z/OS MVS Programming: Authorized Assembler Services Guide	Listening for system events
z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG	*Table: ENF macro event codes*

Network support for z/OS Container Extensions

z/OS V2R4 Communications Server has added network support for z/OS Container Extensions.

z/OS Container Extensions provides native z/OS support for Linux Docker based application workloads. The Communications Server support provides network support for z/OS Container Extensions workloads by introducing a new type of DVIPA called a zCX DVIPA. The zCX DVIPA represents an instance of a Docker server allowing TCP/IP to provide unique IP routing and apply various TCP/IP QoS functions for container workloads running within each Docker server address space.

The Communications Server VTAM support introduces a new type of zCX network transport that dynamically provides optimized internal network connectivity from each Docker server address space ID (ASID) to TCP/IP for providing access to and from the external network. The VTAM support also introduces the z/OS Container Extensions Direct Network Interface Component (DNIC) that provides a Virtual NIC for the Docker server virtualization environment.

Using network support for z/OS Container Extensions

To enable network support for z/OS Container Extensions, perform the tasks in Table 109 on page 117.

Table 109. Task topics to enable network support for z/OS Container Extensions	
Task/Procedure	**Reference**
Use the z/OSMF workflows to create the zCX environment.	z/OS Upgrade Workflow
Generate the TCP/IP Docker Server interfaces.	Configure a DYNAMICXCF and/or DYNAMICXCF6 statement in z/OS Communications Server: IP Configuration Reference
Configure the VIPARANGE ZCX DVIPA address and start the TCP/IP Docker Server interface.	VIPADYNAMIC - VIPARANGE statement in z/OS Communications Server: IP Configuration Reference

To find all related topics about network support for z/OS Container Extensions, see Table 110 on page 117.

Table 110. All related topics about network support for z/OS Container Extensions	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• IBM z/OS Container Extensions network overview • Configuring application-instance DVIPAs for IBM z/OS Container Extensions (zCX) • Connectivity and gateway functions • Terminology • Introduction to VIPA • Configuring DVIPA support

Table 110. All related topics about network support for z/OS Container Extensions (continued)	
Book name	**Topics**
z/OS Communications Server: IP Configuration Reference	• VIPADYNAMIC - VIPARANGE statement
z/OS Communications Server: IP Programmer's Guide and Reference	• Interface statistics record (subtype 6) • TCP/IP profile record dynamic VIPA (DVIPA) address section
z/OS Communications Server: IP System Administrator's Commands	• Netstat VIPADyn/-v report • Netstat VIPADCFG/-F report
z/OS Communications Server: IP and SNA Codes	Data link control (DLC) status codes
z/OS Communications Server: SNA Operation	• DISPLAY ID command • DISPLAY TRL command • MODIFY TRACE command • MODIFY VTAMOPTS command • START command
z/OS Communications Server: SNA Network Implementation Guide	• Resources automatically activated by VTAM
z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures	• I/O trace
z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT	• AFSM entry for altering an FSM state • DNIx entry for recording DNI events • DNI2 entry for continued recording of DNI events • DNI3 entry for continued recording of DNI events • IUTx entry for IUT processing (Part 1) – IUTZ mapping and field descriptions • Trace options for the VIT • TSNS entry to trace sense codes
z/OS Communications Server: SNA Resource Definition Reference	• INOPDUMP start option
z/OS Communications Server: Quick Reference	• D TRL command • F VTAMOPTS command • Start options
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD0007I • EZD0009I • EZD2045I

Table 110. All related topics about network support for z/OS Container Extensions (continued)	
Book name	**Topics**
z/OS Communications Server: SNA Messages	• IST087I • IST1717I • IST2447I • IST2448I • IST2449I • IST2450I • IST2451I • IST2452I • IST2453I • IST2454I • IST2455E • IST2456I

IWQ support for IPSec

z/OS V2R4 Communications Server is enhanced to support inbound workload queueing for IPSec workloads for OSA-Express in QDIO mode.

Inbound workload queueing uses multiple input queues for each QDIO data device (subchannel device) to improve TCP/IP stack scalability and general network optimization. To implement the performance improvements for IPSec workloads, enable inbound workload queueing to process IPSec, EE, sysplex distributor, and streaming bulk data traffic all concurrently with other types of inbound QDIO traffic. When you enable these improvements for a QDIO interface, inbound IPSec, EE, sysplex distributor, and streaming bulk data traffic are each processed on their own ancillary input queue (AIQ). All other inbound traffic is processed on the primary input queue.

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

Dependencies:

- This function is limited to OSA-Express6S Ethernet features or later in QDIO mode running on IBM z14. For more information about the QDIO inbound workload queueing function and the OSA-Express features that support it, see QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide. See the 3906DEVICE or 3907DEVICE Preventive Service Planning (PSP) bucket for more information.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

Using IWQ support for IPSec

To enable IWQ support for IPSec, complete the appropriate tasks in Table 111 on page 120.

Table 111. Task topics to enable IWQ support for IPSec	
Task	**Reference**
Enable inbound workload queueing for a specific QDIO interface by specifying the WORKLOADQ parameter on the IPAQENET or IPAQENET6 INTERFACE statement (if not already configured).	• See the following statements in z/OS Communications Server: IP Configuration Reference: – INTERFACE-IPAQENET OSA-Express QDIO interfaces – INTERFACE-IPAQENET6 OSA-Express QDIO interfaces • Steps for enabling QDIO inbound workload queueing in z/OS Communications Server: IP Configuration Guide
Display whether inbound workload queueing is in effect for the QDIO interface by issuing the **Netstat DEvlinks/-d** command.	Netstat DEvlinks/-d report in z/OS Communications Server: IP System Administrator's Commands
Display whether inbound workload queueing is in effect for the QDIO interface and display the workload queueing functions and queue IDs for that interface by issuing the **DISPLAY NET,ID=trle** command or the **DISPLAY NET,TRL,TRLE=trle** command.	See the following topics in z/OS Communications Server: SNA Operation: • DISPLAY ID command • DISPLAY TRL command
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by initiating VTAM tuning statistics for the QDIO interface.	MODIFY TNSTAT command in z/OS Communications Server: SNA Operation
Monitor whether inbound traffic is using inbound workload queueing and display statistics for each queue by using the TCP/IP callable NMI GetIfStatsExtended request.	TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer's Guide and Reference
Determine the QID on which a specific packet was received, and the associated workload queueing function, from a packet trace.	Formatting packet traces using IPCS in z/OS Communications Server: IP Diagnosis Guide
Determine the QID on which a specific packet was received from an OSAENTA trace.	Formatting OSA traces using IPCS in z/OS Communications Server: IP Diagnosis Guide

To find all related topics about IWQ support for IPSec, see Table 112 on page 120.

Table 112. All related topics about IWQ support for IPSec	
Book name	**Topics**
IP Configuration Guide	• QDIO inbound workload queueing
IP Configuration Reference	• INTERFACE-IPAQENET OSA-Express QDIO interfaces • INTERFACE-IPAQENET6 OSA-Express QDIO interfaces
IP Programmer's Guide and Reference	• TCP/IP callable NMI (EZBNMIFR)
IP Diagnosis Guide	• Formatting packet traces using IPCS • Formatting OSA traces using IPCS

Table 112. All related topics about IWQ support for IPSec (continued)	
Book name	**Topics**
IP System Administrator's Commands	• DISPLAY TCPIP,,OSAINFO • Netstat DEvlinks/-d report
SNA Operations	• DISPLAY ID command • DISPLAY TRL command • MODIFY TNSTAT command
SNA Messages	• IST1221I • IST1230I

Enhancing security

The following topics describe enhancements for security:

Support for SMF compliance evidence

z/OS V2R4 Communications Server with APAR PH37372 generates new SMF type 1154 records that provide compliance evidence for the TCP/IP stack (subtype 1), FTP daemon (subtype 2), TN3270E Telnet server (subtype 3), and CSSMTP client (subtype 4).

This data can be helpful in determining compliance with various industry regulations and standards.

These records are generated whenever an Event Notification Facility (ENF) 86 signal is emitted by a system in the sysplex and the ENF 86 parameter list includes the local z/OS system name. The ENF 86 signal is triggered by a z/OSMF Compliance REST API.

Restriction: z/OS APARs OA61443 and OA61444 are required to support the new ENF 86 signal.

Dependencies:

- The TCP/IP stack must be active to provide the TCP/IP stack compliance evidence SMF record.
- The FTP daemon must be active to provide the FTP daemon compliance evidence SMF record.
- The TN3270E Telnet server must be active to provide TN3270E Telnet server compliance evidence SMF records (one per server port).
- CSSMTP must be active to provide the CSSMTP client compliance evidence record.

Using Support for SMF compliance evidence

To use Support for SMF compliance evidence, complete the appropriate tasks in Table 113 on page 122.

Table 113. Task topics to enable Support for SMF compliance evidence

Task	Reference
Review the data provided in the SMF 1154 records.	• SMF type 1154 records and Appendix F. Type 1154 SMF records in z/OS Communications Server: IP Programmer's Guide and Reference • Assembler mapping macro EZASM482 can be found in SYS1.MACLIB • C header mapping file can be found in SEZANMAC(EZA482) or /usr/include/eza482.h

To find all related topics about Support for SMF compliance evidence, see Table 114 on page 122.

Table 114. All related topics about Support for SMF compliance evidence

Book name	Topics
z/OS Communications Server: IP Configuration Guide	Accounting - SMF records
z/OS Communications Server: IP Programmer's Guide and Reference	• SMF records • SMF type 1154 records • Appendix F. Type 1154 SMF records
z/OS Release Upgrade Reference Summary	• New and changed System Management Facilities (SMF) records for z/OS V2R4 • New and changed members in SYS1.MACLIB for z/OS V2R4

FTP server JES access control

z/OS V2R4 Communications Server, with APAR PH42618, supports a new SAF resource in the SERVAUTH class to control which users are allowed to access FTP JES mode. When the SERVAUTH class is active and a profile is defined for the EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES SAF resource, only users with permission to the profile are allowed to access FTP JES mode.

Dependency: The SERVAUTH class must be active for the EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES SAF resource to provide access controls.

Using FTP server JES access control

To use FTP server JES access control, complete the appropriate tasks in Table 115 on page 123.

Table 115. Task topics to enable FTP server JES access control

Task	Reference
Implement FTP JES access controls using the SERVAUTH class • Activate the SERVAUTH class, if it is not already active. • Define an EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES SAF resource profile with UACC(NONE). • For each user that should be allowed to use FTP FILETYPE=JES, give the user READ permission to the defined profile.	(Optional) Steps for controlling user access to FTP JES mode in z/OS Communications Server: IP Configuration Guide

To find all related topics about FTP server JES access control, see Table 116 on page 123.

Table 116. All related topics about FTP server JES access control

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Local user access control to TCP/IP resources using SAF • Security for the FTP server • (Optional) Steps for controlling user access to FTP JES mode • Customizing the FTP-to-JES interface for JESINTERFACELevel 2 (optional)
z/OS Communications Server: IP Configuration Reference	• FILETYPE (FTP client and server) statement
z/OS Communications Server: IP User's Guide and Commands	• Restricting access to FTP JES mode with SAF profiles • JES security using JESINTERFACELEVEL 2 • Changing JESSTATUS, JESOWNER, and JESJOBNAME
z/OS Communications Server: IP and SNA Codes	• 200-: User *user_name* is not allowed to use FILETYPE=JES

IBM zERT Network Analyzer passphrase and password management support

The IBM zERT Network Analyzer with APAR PH43119 for z/OS V2R4 supports the use of passphrases up to 100 characters to connect to the Db2 for z/OS database. The IBM zERT Network Analyzer includes additional enhancements in the **Database Settings** panel to clear existing database credentials to allow for easier switching to a different database user ID.

Using IBM zERT Network Analyzer passphrase and password management support

To use IBM zERT Network Analyzer passphrase and password management support, perform the tasks in Table 117 on page 124.

Table 117. IBM zERT Network Analyzer passphrase and password management support	
Task/Procedure	**Reference**
Configure the passphrase for the IBM zERT Network Analyzer database	See *Working with the Database Settings panel* of *IBM zERT Network Analyzer online help*, Analysis category under the IBM z/OS Management Facility online help
Clear the existing saved IBM zERT Network Analyzer database	See *Working with the Database Settings panel* of *IBM zERT Network Analyzer online help*, Analysis category under the IBM z/OS Management Facility online help

To find all related topics about IBM zERT Network Analyzer passphrase and password management support, see Table 118 on page 124.

Table 118. All related topics about IBM zERT Network Analyzer passphrase and password management support	
Book name	**Topics**
z/OS Management Facility online help	IBM zERT Network Analzyer online help

IBM Health Checker for use of native TLS/SSL support for DCAS

z/OS V2R4 Communications Server, with TCP/IP APAR PH16144 and SNA APAR OA58255, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies if DCAS uses native TLS/SSL support.

Dependency: You must install TCP/IP APAR PH16144 and SNA APAR OA58255 and start the IBM Health Checker for z/OS to use the new migration health check.

Using the IBM Health Checker for use for native TLS/SSL support for DCAS

To use the IBM Health Checker for z/OS migration health check support, perform the tasks in Table 119 on page 124.

Table 119. IBM Health Checker for use of native TLS/SSL support for DCAS	
Task/Procedure	**Reference**
To use the new migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL migration health check. 3. Review health check output for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for use of native TLS/SSL support for DCAS, see Table 120 on page 124.

Table 120. All related topics about IBM Health Checker for use of native TLS/SSL support for DCAS	
Book name	**Topics**
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL

Table 120. All related topics about IBM Health Checker for use of native TLS/SSL support for DCAS (continued)	
Book name	**Topics**
z/OS Upgrade Workflow	*IP Services: Migrate TLS/SSL support for DCAS to AT-TLS*
z/OS Communications Server: SNA Messages	• ISTM043I • ISTM044E

IBM Health Checker for use of native TLS/SSL support for the FTP server

z/OS V2R4 Communications Server, with TCP/IP APAR PH21573 and SNA APAR OA59022, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies active FTP servers using native TLS/SSL support.

z/OS V2R4 Communications Server, with TCP/IP APAR PH24732 and SNA APAR OA59490, provides additional migration health checks to use with the IBM Health Checker for z/OS function. These migration health checks identify FTP servers and clients that are configured with an invalid configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS.

Dependencies:

- You must install TCP/IP APAR PH21573 and SNA APAR OA59022 and start the IBM Health Checker for z/OS to use the new migration health check to identify active FTP servers using native TLS/SSL support.
- You must install TCP/IP APAR PH24732 and SNA APAR OA59490 and start the IBM Health Checker for z/OS to use the new migration health checks to identify FTP servers and clients that are configured with an invalid configuration of TLSRFCLEVEL CCCNONOTIFY with TLSMECHANISM ATTLS.

Using the IBM Health Checker for use of native TLS/SSL support for the FTP server.

To use the IBM Health Checker for z/OS migration health check support, perform the tasks in Table 121 on page 125.

Table 121. IBM Health Checker for use of native TLS/SSL support for the FTP server	
Task/Procedure	**Reference**
To use the new migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL FTP server migration health check. 3. Activate the ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL FTP server migration health check. 4. Activate the ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL FTP client migration health check. 5. Review health check output for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for use of native TLS/SSL support for the FTP server, see Table 122 on page 126.

Table 122. All related topics about IBM Health Checker for use of native TLS/SSL support for the FTP server	
Book name	**Topics**
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
z/OS Communications Server: IP Configuration Guide	• Steps for customizing the FTP server for TLS • Steps for migrating the FTP server and client to use AT-TLS
IBM Health Checker for z/OS: User's Guide	• ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL • ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL • ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL
z/OS Upgrade Workflow	• *IP Services: Migrate TLS/SSL support for FTP server to AT-TLS* • *IP Services: Ensure FTP servers and FTP clients are not configured with TLSRFCLEVEL CCCNONOTIFY and TLSMECHANISM ATTLS*
z/OS Communications Server: SNA Messages	• ISTM045I • ISTM046E • ISTM047I • ISTM048E • ISTM049I • ISTM050E
z/OS Communications Server: IP Messages Volume 3 (EZY)	• EZYFT79I • EZYFT88I

IBM Health Checker for use of native TLS/SSL support for the TN3270 server

z/OS V2R4 Communications Server, with TCP/IP APAR PH16144 and SNA APAR OA58255, provides a new migration health check to use with the IBM Health Checker for z/OS function. The migration health check identifies active TN3270 servers using native TLS/SSL support.

Dependency: You must install TCP/IP APAR PH16144 and SNA APAR OA58255 and start the IBM Health Checker for z/OS to use the new migration health check.

Using the IBM Health Checker for use for native TLS/SSL support for the TN3270 server

To use the IBM Health Checker for z/OS migration health check support, perform the tasks in Table 123 on page 127.

Table 123. IBM Health Checker for use of native TLS/SSL support for the TN3270 server	
Task/Procedure	**Reference**
To use the new migration health check, take the following steps: 1. Configure and start the IBM Health Checker for z/OS. 2. Activate the ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL migration health check. 3. Review health check output for potential migration actions.	See the following topics in IBM Health Checker for z/OS: User's Guide: • Setting up IBM Health Checker for z/OS • Working with check output • Managing checks

To find all new and updated topics about IBM Health Checker for use of native TLS/SSL support for the TN3270 server, see Table 124 on page 127.

Table 124. All related topics about IBM Health Checker for use of native TLS/SSL support for the TN3270 server	
Book name	**Topics**
z/OS Communications Server: IP Diagnosis Guide	IBM Health Checker for z/OS
IBM Health Checker for z/OS: User's Guide	ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL
z/OS Upgrade Workflow	*IP Services: Migrate TLS/SSL support for TN3270 to AT-TLS*
z/OS Communications Server: SNA Messages	• ISTM041I • ISTM042E

Sysplex Autonomics for IPSec

z/OS V2R4 with APAR PH12788 enhances the sysplex autonomics function to monitor IPsec infrastructure. You can request that sysplex autonomics delay a TCP/IP stack from joining a sysplex group until the IPsec infrastructure is active. You can also request that sysplex autonomics monitor the IPsec infrastructure after the stack has joined the sysplex group. If monitoring the IPsec infrastructure is enabled, you are alerted with new messages when the IPsec infrastructure is not operational. You can optionally configure the TCP/IP stack to also take a recovery action and leave the sysplex when it detects that the IPsec infrastructure is not active. This allows a backup TCP/IP stack to take over DVIPAs from the system that left the sysplex.

Restrictions:

- The monitoring of the IPsec infrastructure can only be enabled for a TCP/IP stack that is using sysplex-wide security sessions (SWSA) and has the DVIPSEC parameter configured on the IPSEC statement in the TCP/IP profile.
- While the EZBDVIPA coupling facility structure is required for IPsec sysplex-wide security associations (SWSA), the ability of the TCP/IP stack to connect to or access the EZBDVIPA structure is not monitored by sysplex autonomics for IPsec. A failure related to the EZBDVIPA structure would typically be sysplex-wide. It would not be beneficial for a TCP/IP stack to leave the sysplex for a sysplex-wide failure.
- In IPsec configurations where both a primary and backup NSSD are configured for certificate services, no monitoring of the IKED connection to NSSD is done after the TCP/IP stack joins the sysplex. See the IP Configuration Guide “Sysplex Autonomics for IPsec infrastructure” for additional information.

Incompatibilities:

- If your IPsec infrastructure includes the Network Security Services daemon (NSSD), and the IKED to NSSD connection uses a DVIPA as the source or destination IP address, the sysplex autonomics IPsec infrastructure monitoring function should not be enabled.
- If you use a centralized Policy Agent server for IPsec or AT-TLS policy, and the connection from the policy client to the policy server uses a DVIPA as the source or destination IP address, the sysplex autonomics IPsec infrastructure monitoring function should not be enabled.

Note: With APAR PH16303, you can configure this function in Network Configuration Assistant (NCA).

Using Sysplex Autonomics for IPSec

To enable Sysplex Autonomics for IPSec, perform the tasks in Table 125 on page 128.

Table 125. Sysplex Autonomics for IPSec

Task/Procedure	Reference
Enable monitoring of the IPsec infrastructure by sysplex autonomics with the GLOBALCONFIG SYSPLEXMONITOR sub-parameters DELAYJOINIPSEC and MONIPSEC	• GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference • Sysplex problem detection and recovery topic in z/OS Communications Server: IP Configuration Guide
Display sysplex autonomics configuration settings	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
(Optional) Configure the NoKeyring parameter on the IkeConfig statement in the IKE configuration file, if appropriate. If an IKE key ring is not explicitly configured, the Keyring parameter defaults to iked/keyring. If there is no keyring for IKED to process, you can specify NoKeyring.	IkeConfig statement in z/OS Communications Server: IP Configuration Reference
Display the IKED configuration parameters	MODIFY command: IKE server in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about Sysplex Autonomics for IPSec, see Table 126 on page 128.

Table 126. All related topics about Sysplex Autonomics for IPSec

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Sysplex problem detection and recovery • Problem detection • Recovery • Summary of problems monitored and actions taken • Sysplex autonomics for IPsec
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement • IkeConfig statement

Table 126. All related topics about Sysplex Autonomics for IPSec (continued)	
Book name	**Topics**
z/OS Communications Server: IP System Administrator's Commands	• Not IPv6 enabled (SHORT format) • IPv6 enabled or request for LONG format • Report field descriptions • VARY TCPIP,,SYSPLEX Parameters • Netstat CONFIG/-f report • MODIFY command: IKE server
z/OS Communications Server: IP Programmer's Guide and Reference	TCP/IP profile record Global configuration section
z/OS Communications Server: IP Diagnosis Guide	Sample output of the TCPIPCS PROFILE subcommand
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD1976E • EZD1977E • EZD1979E • EZD2048I • EZD2049I • EZD2050I
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	EZZ0839I

IBM zERT Network Analyzer database administration enhancements

z/OS Management Facility (z/OSMF) V2R4 with the IBM zERT Network Analyzer APAR PH24494 provides additional flexibility in IBM zERT Network Analyzer's Db2 for z/OS database schema definitions and reduces the access privileges required by the IBM zERT Network Analyzer's database user ID. The supplied database schema tooling now supports customized values for the database schema name, index names and even table names along with many other operational parameters that were already configurable.

Dependencies: No new dependencies are introduced. The IBM zERT Network Analyzer requires z/OSMF to be installed and a type 4 JDBC connection to Db2 for z/OS 11 or higher.

Using IBM zERT Network Analyzer database administration enhancements

To enable IBM zERT Network Analyzer database administration enhancements, perform the tasks in Table 127 on page 129.

Table 127. IBM zERT Network Analyzer database administration enhancements	
Task/Procedure	**Reference**
Stop z/OSMF if it is running	

Table 127. IBM zERT Network Analyzer database administration enhancements (continued)	
Task/Procedure	**Reference**
• If you are installing the IBM zERT Network Analyzer for the first time, your Db2 for z/OS database administrator (DBA) will need to create your customized database using the provided schema tooling. • If you already have the IBM zERT Network Analyzer running: – Your DBA needs to either upgrade the existing database schema to the new schema version or else drop your existing database and re-create it with customized schema, index and/or table names at the new schema version. – Regardless of which approach you decide, your DBA uses the provided database schema tooling to implement the changes. This includes deciding on and defining the desired number of IBM zERT Network Analyzer query result table partitions.	See Db2 for z/OS customization for the IBM zERT Network Analyzer task in IBM z/OS Management Facility Configuration Guide
Once the IBM zERT Network Analyzer database is updated to or created at the new schema version , start z/OSMF and the IBM zERT Network Analyzer plugin. If you are using a newly created database, you need to fill in and save the required JDBC connectivity settings in the IBM zERT Network Analyzer's database settings panel.	See Connect the IBM zERT Network Analyzer task with the Db2 for z/OS database in IBM z/OS Management Facility Configuration Guide
Once the correct database settings are stored and the IBM zERT Network Analyzer successfully connects to the database, you can verify the database schema information in the database settings panel.	See *Working with the Database Settings panel* of IBM zERT Network Analyzer online help, *Analysis* category under the IBM z/OS Management Facility online help
(Optionally) Configure the report timeout value to specify how many minutes of inactivity will result in the report being closed and the associated query result table partition being made available for future query requests.	IBM zERT Network Analyzer online help
(Optionally) Configure the maximum number of reports a single user can have concurrently open.	IBM zERT Network Analyzer online help

To find all related topics about IBM zERT Network Analyzer database administration enhancements, see Table 128 on page 130.

Table 128. All related topics about IBM zERT Network Analyzer database administration enhancements	
Book name	**Topics**
IBM z/OS Management Facility Configuration Guide	• Updating z/OS for the IBM zERT Network Analyzer plug-in • Db2 for z/OS customization for the IBM zERT Network Analyzer task • Recovering unavailable partition
z/OS Management Facility online help	IBM zERT Network Analzyer online help

AT-TLS support for TLS v1.3

z/OS V2R4 Communications Server adds support for TLS Version 1.3 for Application Transparent Transport Layer Security (AT-TLS). This includes support for the following new TLSv1.3 cipher suites: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, and TLS_CHACHA20_POLY1305_SHA256.

z/OS V2R4 Communications Server enhances the z/OS Encryption Readiness Technology (zERT) function to detect and report TLSv1.3 security session information using SMF Type 119 subtype 11 and 12 records. The IBM zERT Network Analyzer z/OSMF plug-in is also enhanced to accept and display TLSv1.3 information and to allow IBM zERT Network Analyzer users to query database content using the new TLSv1.3 security session characteristics.

Be aware that the CPU consumption of the TCP/IP address space will increase when you enable TLSv1.3. While TLSv1.3 provides stronger cryptographic protection for your TCP connections, it inherently uses more cryptographic operations and therefore consumes more CPU than TLSv1.2 when using comparable cipher suites and key exchange algorithms. In addition, TLSv1.3 uses some algorithms that are new in z/OS V2R4 and are implemented in software only (without any hardware acceleration). The most significant of these is the new RSASSA-PSS signature algorithm, which is required if you use RSA certificates.

The magnitude of the CPU increase depends on a variety of factors, including the cipher suites you were using under TLSv1.2 (or earlier) and the level of hardware you are using (in the z15 and later models, CPACF acceleration of ECC operations can benefit TLSv1.3 performance).

The TLSv1.3 support in V2R4 System SSL can be used for production workloads as long as you understand these performance considerations. A decision to move to TLSv1.3 should be based on the extra security that protocol provides and with the understanding that the extra security comes with a noticeable CPU cost.

Restrictions:

Support for TLS Version 1.3 is provided only for AT-TLS. Native TLS support for the FTP server and client, the TN3270E server, and DCAS is not updated to support TLSv1.3.

Incompatibilities:

- The cipher suites supported for TLS Version 1.2 and earlier are not supported for TLS Version 1.3. And the cipher suites supported for TLS Version 1.3 are not supported by earlier versions of TLS. If TLSv1.3 and earlier versions are enabled, the configured list of supported cipher suites must include values supported for TLSv1.3 and values supported by earlier TLS versions.
- The FIPS 140-2 standard does not define support for TLSv1.3 or the new cipher suites defined for it. Enabling both the TLSv1.3 protocol and FIPS support results in an error.

Dependency:

The Integrated Cryptographic Services Facility (ICSF) must be active to provide support for all TLSv1.3 cipher suites.

Using AT-TLS support for TLS v1.3

To enable AT-TLS support for TLS v1.3, perform the tasks in Table 129 on page 132.

Table 129. AT-TLS support for TLS v1.3	
Task/Procedure	**Reference**
Enable TLS v1.3 in AT-TLS policy by using the Network Configuration Assistant (NCA) or manual configuration.	See the following topics: • IBM Configuration Assistant for z/OS Communications Server online helps • AT-TLS policy statements in z/OS Communications Server: IP Configuration Reference • Using TLSv1.3 protocol support in z/OS Communications Server: IP Configuration Guide
Optionally, display the policy-based networking information. Use the pasearch command to display AT-TLS policies.	The z/OS UNIX pasearch command: Display policies in z/OS Communications Server: IP System Administrator's Commands
Optionally, display the AT-TLS negotiated and configured parameters in use for a TCP connection.	Netstat TTLS/-x reportin z/OS Communications Server: IP System Administrator's Commands
Optionally, view updated AT-TLS information in the following SMF type 119 records: • TCP connection termination record (subtype 2) • FTP records, including: – subtype 3 – subtype 70 – subtype 100 – subtype 101 – subtype 102 – subtype 103 – subtype 104 • zERT connection detail record (subtype 11) • zERT connection summary record (subtype 12) • CSSMTP connection record (subtype 49)	Type 119 SMF records in z/OS Communications Server: IP Programmer's Guide and Reference
Optionally, retrieve updated AT-TLS information for a connection with the TCP/IP callable NMI (EZBNMIFR).	TCP/IP callable NMI (EZBNMIFR) in z/OS Communications Server: IP Programmer's Guide and Reference

To find all related topics about AT-TLS support for TLS v1.3, see Table 130 on page 132.

Table 130. All related topics about AT-TLS support for TLS v1.3	
Book name	**Topics**
z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference	• IOCTL • Sockets return codes (ERRNOs)
z/OS Communications Server: IP CICS Sockets Guide	Sockets return codes (ERRNOs)
z/OS Communications Server: IP IMS Sockets Guide	Sockets return codes (ERRNOs)
z/OS Communications Server: IP Messages Volume 2 (EZB, EZD)	• EZD1282I • EZD1283I • EZD1286I

Table 130. All related topics about AT-TLS support for TLS v1.3 (continued)

Book name	Topics
z/OS Communications Server: IP Programmer's Guide and Reference	• zERT connection detail record (subtype 11) • zERT Summary record (subtype 12) • Application Transparent Transport Layer Security (AT-TLS) • CICS transaction considerations • Starting AT-TLS on a connection • Steps for implementing a controlling server application • SIOCTTLSCTL ioctl return values • TCP connection termination record (subtype 2) • FTP client transfer completion record (subtype 3) • FTP server transfer completion record (subtype 70) • FTP server logon failure record (subtype 72) • z/OS Communications Server: IP Programmer's Guide and Reference • FTP client transfer initialization record (subtype 101) • FTP client login failure record (subtype 102) • FTP client session record (subtype 103) • FTP server session record (subtype 104) • FTP client application data format for the control connection • FTP client application data format for the data connection • FTP server application data format for the control connection • FTP server application data format for the data connection • Application data format for CSSMTP • Application data format for Telnet • Type 119 SMF records • TCP/IP callable NMI (EZBNMIFR)
z/OS Communications Server: IP System Administrator's Commands	• COnn report examples • Report field descriptions • The z/OS UNIX pasearch command: Display policies

Table 130. All related topics about AT-TLS support for TLS v1.3 (continued)	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Security • Existing workload • TLS and SSL • TN3270E Telnet server security • Multiple port support • Secure and non-secure connections using a single Telnet port • Express Logon Feature • Application Transparent Transport Layer Security • Cipher suite specification • Protocol versions • Using TLSv1.3 protocol support • Certificate validation • Encryption key refresh • Handshake timer • Wireless performance • Certificate selection • Session caching • AT-TLS access control considerations • Client application model • What are the limitations for zERT discovery? • AT-TLS controlling application considerations • Client application model • Server application model • Forked server application model
z/OS Communications Server: IP Configuration Reference	• TTLSConnectionAdvancedParms statement • TTLSEnvironmentAction statement • TTLSEnvironmentAdvancedParms statement • TTLSSignatureParms statement • TTLSGskAdvancedParms statement • TTLSCipherParms statement • TTLSGskOcspParms statement • General syntax rules for Policy Agent • AT-TLS policy statements

z/OS Encryption Readiness Technology (zERT) aggregation

z/OS V2R3 Communications Server, introduced a new function called z/OS Encryption Readiness Technology (zERT). With zERT, the TCP/IP stack acts as a focal point in collecting and reporting the cryptographic security attributes of IPv4 and IPv6 application traffic that is protected using the TLS/SSL, SSH, and IPSec cryptographic network security protocols. The collected connection level data is written to SMF in SMF 119 subtype 11 records.

In certain environments, the volume of SMF 119 subtype 11 records can be large. z/OS V2R4 Communications Server provides the zERT aggregation function. The zERT aggregation function provides an alternative SMF view of the collected security session data. This alternate view is written in the form of new SMF 119 subtype 12 records that summarize the use of security sessions by many application connections over time and which are written at the end of each SMF/INTVAL interval. This alternate view condenses the volume of SMF record data while still providing all the critical security information.

Decreasing the frequency at which zERT summary records are written may increase the amount of 64-bit pageable, private memory needed, because the zERT aggregation information is held longer in memory before being written out to SMF.

Restrictions:

The following restrictions apply to both zERT discovery and zERT aggregation functions.

- zERT collects information for TCP and Enterprise Extender (EE) connections. Information is not collected for non-EE UDP traffic or traffic using other IP protocols.
- zERT collects cryptographic security attributes for the TLS, SSL, SSH, and IPSec protocols. No other cryptographic security protocols are supported.
- The following z/OS cryptographic protocol providers are fully enabled for zERT: z/OS Communications Server IPSec and AT-TLS, z/OS Cryptographic Services System SSL, and z/OS OpenSSH. Detailed security attribute data is available for connections using these protocol providers. Other TLS, SSL, and SSH implementations running on z/OS are monitored through stream observation only. A limited amount of security attribute data is available for these connections.
- The interval at which the SMF 119 subtype 12 records are created will be determined by the ZERT AGGregation sub-parameter INTVAL. (INTVAL/SYNCVAL sub-parameters are available in z/OS V2R4 Communications Server with APAR PH25049.)
- For information on the specific cases where security attribute data is limited or unavailable, see What are the limitations for zERT discovery? in z/OS Communications Server: IP Configuration Guide.

Dependency: In order to properly monitor IBM Sterling Connect:Direct traffic when it is protected through SecurePlus TLS/SSL support, you must apply Connect:Direct APAR PI77316.

Using z/OS Encryption Readiness Technology (zERT) aggregation

To enable z/OS Encryption Readiness Technology (zERT) aggregation, perform the tasks in Table 131 on page 135.

Table 131. zERT aggregation

Task/Procedure	Reference
Plan for collection and storage of zERT summary SMF records and decide whether or not you want to discontinue collection of zERT connection detail records.	• Monitoring cryptographic network protection: z/OS encryption readiness technology (zERT) in z/OS Communications Server: IP Configuration Guide • z/OS MVS System Management Facilities (SMF)
Enable the zERT aggregation function.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
If you want zERT summary records to be available in the System Management Facility data sets or log streams, specify SMFCONFIG TYPE119 ZERTSUMMARY.	• SMFCONFIG statement in z/OS Communications Server: IP Configuration Reference

Table 131. zERT aggregation (continued)	
Task/Procedure	**Reference**
If you want zERT summary records to be available to a real-time NMI application: • Perform the necessary RACF processing to authorize the NMI application to use the zERT Summary SMF NMI service (SYSTCPES). • Specify NETMONITOR ZERTSUMMARY in the TCP/IP profile.	• Requests sent by the client to the server: SYSTCPES service in z/OS Communications Server: IP Programmer's Guide and Reference • NETMONITOR statement in z/OS Communications Server: IP Configuration Reference
Display zERT aggregation configuration settings	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands
Enable the zERT aggregation INTVAL and SYNCVAL.	GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference
Display zERT aggregation INTVAL and SYNCVAL configuration settings.	Netstat CONFIG/-f report in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about zERT aggregation, see Table 132 on page 136.

Table 132. All related topics about zERT aggregation	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• Monitoring cryptographic network protection: z/OS encryption readiness technology (zERT) • What are the limitations for zERT discovery? • What does zERT aggregation collect? • How does zERT aggregation summarize the information? • How does zERT aggregation provide the information? • How does zERT aggregation determine the server port? • Using z/OS Encryption Readiness Technology (zERT) • Enabling zERT discovery • Enabling zERT aggregation • Enabling a longer zERT aggregation recording interval • Selecting a destination for zERT discovery SMF records • Selecting a destination for zERT aggregation SMF records • Disabling zERT discovery • Disabling zERT aggregation
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement • SMFCONFIG statement • NETMONITOR statement

Table 132. All related topics about zERT aggregation (continued)	
Book name	**Topics**
z/OS Communications Server: IP System Administrator's Commands	• Netstat CONFIG/-f report
z/OS Communications Server: IP Programmer's Guide and Reference	• Real-time TCP/IP network monitoring NMI • Connecting to the AF_UNIX stream socket • Authorizing the applications • Real-time NMI: Connecting to the server • Real-time NMI: Interacting with the servers • Real-time NMI: Common record header • Real-time NMI: Requests sent by the client to the server • Requests sent by the client to the server: SYSTCPES service • Records sent by the server to the client: Initialization record • Records sent by the server to the client: Token record • EZBTMIC1 or EZBTMIC4 parameters • Processing the cte records for SYSTCPER • Processing the cte records for SYSTCPES • SMF type 119 records • TCP/IP profile record Global configuration section • TCP/IP profile record management section • zERT Summary record (subtype 12)

IBM zERT Network Analyzer

IBM zERT (z/OS Encryption Readiness Technology) Network Analyzer is a web-based graphical user interface that z/OS network security administrators can use to analyze and report on data reported in zERT Summary records.

z/OS V2R3 Communications Server introduced a new feature called z/OS Encryption Readiness Technology (zERT). zERT positions the TCP/IP stack to act as a focal point for collecting and reporting the cryptographic security attributes of IPv4 and IPv6 TCP and Enterprise Extender (EE) connection traffic that is protected using the TLS/SSL, SSH and IPSec cryptographic network security protocols. Connection data is written to z/OS System Management Facility (SMF) in two new SMF type 119 records:

- zERT Connection Detail (subtype 11) records are written on a per-connection basis to record the cryptographic protection history of a given TCP or EE connection.
- zERT Summary (subtype 12) records are written on a per-security-session basis at the end of each SMF interval to summarize the repeated use of security sessions during the interval.

A new z/OS Management Facility (z/OSMF) plug-in named IBM zERT Network Analyzer is available with z/OSMF V2R4. IBM zERT Network Analyzer is a web-based graphical user interface that z/OS network security administrators can use to analyze and report on data reported in zERT Summary records.

To get a quick start with IBM zERT Network Analyzer, see IBM zERT Network Analyzer tutorial.

Dependency:

- The IBM zERT Network Analyzer task requires either Db2 11 for z/OS or Db2 12 for z/OS.

Using IBM zERT Network Analyzer

To enable IBM zERT Network Analyzer, perform the tasks in Table 133 on page 138.

Table 133. IBM zERT Network Analyzer

Task/Procedure	Reference
Enable collection of zERT Summary (SMF Type 119 subtype 12) SMF records • Enable zERT Aggregation function by specifying the GLOBALCONFIG ZERT AGGREGATION statement. • Enable a longer interval at which the SMF 119 subtype 12 (zERT summary) records are created by using the INTVAL sub-parameter of the ZERT AGGregation statement. • Display zERT aggregation INTVAL or SYNCVAL configuration settings. • Direct zERT to write the zERT Summary SMF records to the System Management Facility (SMF) by specifying the SMFCONFIG TYPE119 ZERTSUMMARY statement. • Enable the recording of type 119 records, and optionally define the SMF interval duration, in your SMF parmlib member.	• GLOBALCONFIG statement in z/OS Communications Server: IP Configuration Reference • SMFCONFIG statement in z/OS Communications Server: IP Configuration Reference • z/OS MVS System Management Facilities (SMF)
Dump the collected zERT Summary records to a sequential data set using the IFASMFDP or IFASMFDL program • Use IFASMFDP for SMF data sets • Use IFASMFDL for SMF log streams	z/OS MVS System Management Facilities (SMF)
Enable the IBM zERT Network Analyzer plug-in in z/OSMF by adding ZERT_ANALYZER to the PLUGINS statement.	IZUPRMxx reference information in IBM z/OS Management Facility Configuration Guide
Authorize the user IDs that will be using IBM zERT Network Analyzer	Updating z/OS for the IBM zERT Network Analyzer plug-in in IBM z/OS Management Facility Configuration Guide
Create the proper Db2 for z/OS database definitions to use with IBM zERT Network Analyzer	Updating z/OS for the IBM zERT Network Analyzer plug-in in IBM z/OS Management Facility Configuration Guide
Start the z/OSMF IBM zERT Network Analyzer plug-in	*Analysis* category under the IBM z/OS Management Facility online help
Import the dumped zERT SMF Summary records into IBM zERT Network Analyzer	IBM zERT Network Analyzer online help, *Analysis* category under the IBM z/OS Management Facility online help
Analyze the imported zERT Summary data using IBM zERT Network Analyzer query and reporting functions	IBM zERT Network Analyzer online help, *Analysis* category under the IBM z/OS Management Facility online help

To find all related topics about IBM zERT Network Analyzer, see Table 134 on page 139.

Table 134. All related topics about IBM zERT Network Analyzer	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	• z/OS Encryption Readiness Technology (zERT) Concepts • Selecting a destination for zERT aggregation SMF records • Using IBM zERT Network Analyzer
z/OS Communications Server: IP Configuration Reference	• GLOBALCONFIG statement • SMFCONFIG statement
z/OS Communications Server: IP Programmer's Guide and Reference	• zERT connection detail record (subtype 11) • zERT Summary record (subtype 12)
IBM z/OS Management Facility Configuration Guide	• Configure IBM z/OS Encryption Readiness Technology (zERT) Network Analyzer • Updating z/OS for the IBM zERT Network Analyzer Plug-in • Problems when using IBM zERT Network Analyzer • Steps for sending information to IBM Support
IBM zERT Network Analyzer online help	Messages: IZUETXXXXX

TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication

z/OS V2R4 Communications Server, with RACF and IBM MFA for z/OS, extends the TN3270 Telnet server Express Logon Feature (ELF) to support IBM Multi-Factor Authentication (MFA) for z/OS. With this support, TN3270 clients can experience the same single sign-on behavior that is already offered by the PassTicket-based ELF, but now via an MFA token that is assigned by a SAF-compliant external security manager like IBM Security Server RACF. With the new EXPRESSLOGONMFA parameter in the TN3270E Telnet server profile, ELF attempts to authenticate clients by using their X.509 client certificate through MFA. If no MFA token is available for the user, the authentication fails by default. ELF can be configured to revert back to PassTicket authentication in certain cases where MFA authentication is unsuccessful.

Dependencies:

- IBM Security Server RACF
- IBM Multi-Factor Authentication for z/OS

To enable TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication, perform the tasks in Table 135 on page 139.

Table 135. TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication	
Task/Procedure	**Reference**
Define MFA policies for the appropriate client user IDs.	z/OS Security Server RACF Security Administrator's Guide
Enable Express Logon MFA support in the TN3270E Telnet server.	• z/OS Communications Server: IP Configuration Guide • z/OS Communications Server: IP Configuration Reference

To find all related topics about TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication, see Table 136 on page 140.

Table 136. All related topics about TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication

Book name	Topics
z/OS Communications Server: IP Configuration Guide	• Express Logon Feature • Express logon services with the Digital Certificate Access Server • Express Logon Feature – Configuring RACF services for Express Logon – An example of configuring the Express Logon components - Configuring the Host On Demand Telnet client - Configuring the z/OS TN3270E Telnet server (two-tier solution) - Configuring the middle-tier Telnet server (IBM Communications Server for Windows example)
z/OS Communications Server: IP Configuration Reference	• EXPRESSLOGON statement • EXPRESSLOGONMFA statement
z/OS Communications Server: IP Programmer's Guide and Reference	• TN3270E Telnet server profile record TelnetGlobals section • TN3270E Telnet server profile record TelnetParms section
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ6035I • EZZ6060I • EZZ6065I

Application development

The following topics describe enhancements for application development:

SMTPD compatibility enhancements for CSSMTP

z/OS V2R4 Communications Server with APAR PH18237, enhances the Communications Server SMTP (CSSMTP) application with three new configuration parameters to provide better compatibility with SMTPD for your migration from SMTPD to CSSMTP.

Using SMTPD compatibility enhancements for CSSMTP

To enable SMTPD compatibility enhancements for CSSMTP, perform the tasks in Table 137 on page 141.

Table 137. SMTPD compatibility enhancements for CSSMTP	
Task/Procedure	**Reference**
Configure ReportMailFrom to define a default email address for the "Mail From" field in the error report.	ReportMailFrom statement in Communications Server SMTP application in z/OS Communications Server: IP Configuration Reference
Configure ReportSysoutClass to assign a Sysout Class for error reports.	ReportSysoutClass statement in Communications Server SMTP application in z/OS Communications Server: IP Configuration Reference
Configure MailBoxCompatibility to define the mailbox length (Standard or Long).	MailBoxCompatibility statement in Communications Server SMTP application in z/OS Communications Server: IP Configuration Reference
Display the values for the ReportMailFrom, ReportSysoutClass, and MailBoxCompatibility.	MODIFY command: Communications Server SMTP application (CSSMTP) in z/OS Communications Server: IP System Administrator's Commands

To find all related topics about SMTPD compatibility enhancements for CSSMTP, see Table 138 on page 141.

Table 138. All related topics about SMTPD compatibility enhancements for CSSMTP	
Book name	**Topics**
z/OS Communications Server: IP Configuration Guide	Customizing the CSSMTP configuration file to handle undeliverable mail
z/OS Communications Server: IP Configuration Reference	• Communications Server SMTP application – General syntax rules for CSSMTP – CSSMTP configuration statements - MailBoxCompatibility statement - ReportMailFrom statement - ReportSysoutClass statement
z/OS Communications Server: IP System Administrator's Commands	• MODIFY command: Communications Server SMTP application (CSSMTP)

Communications Server resolver enhancements

Starting with z/OS V2R4 Communications Server, users can specify two different maximum TTL values: a new MAXNEGTTL resolver setup statement for negative cache entries and the existing MAXTTL resolver setup statement for all other cache entries.

Prior to V2R4, the resolver caching function provided users with the ability to set a maximum time-to-live (TTL) value for cached Domain Name System (DNS) name server information, but the MAXTTL resolver setup statement applied to all types of cached DNS name server entries.

In addition, the output of the MODIFY RESOLVER,DISPLAY|REFRESH command is enhanced to include the name of the most recently used resolver setup file.

Using Communications Server resolver enhancements

To enable Communications Server resolver enhancements, perform the tasks in Table 139 on page 142.

Table 139. Communications Server miscellaneous enhancements	
Task/Procedure	**Reference**
If you want a maximum time-to-live (TTL) value for negative cache entries that is different from the maximum TTL for other cache entries, add the MAXNEGTTL configuration statement to the resolver setup file.	MAXNEGTTL statement in z/OS Communications Server: IP Configuration Reference
To enable the new value, take one of the following steps: • Start the resolver if it is not running. • If the resolver is running, issue the MODIFY RESOLVER,REFRESH,SETUP=*<setup file name>* command.	MODIFY command: Resolver address spacein z/OS Communications Server: IP System Administrator's Commands

To find all related topics about Communications Server miscellaneous enhancements, see Table 140 on page 142.

Table 140. All related topics about Communications Server miscellaneous enhancements	
Book name	**Topics**
z/OS Communications Server: IP Messages Volume 4 (EZZ, SNM)	• EZZ9293I • EZZ9298I • EZZ9304I
z/OS Communications Server: IP Diagnosis Guide	Interpreting the Trace Resolver output
z/OS Communications Server: IP System Administrator's Commands	• MODIFY command: Resolver address space • DETAIL or DETAIL NEGATIVE reports
z/OS Communications Server: IP Programmer's Guide and Reference	GetResolverConfig response contents
z/OS Communications Server: IP Configuration Reference	• Resolver setup statements • MAXNEGTTL statement • MAXTTL statement
z/OS Communications Server: IP Configuration Guide	• The resolver setup file • Steps for creating a resolver setup file • Information that is cached by the resolver • Steps for configuring resolver caching (optional) • Steps for manually managing the storage capacity of the resolver cache

Code page enhancements for CSSMTP

z/OS V2R4 Communications Server is enhanced to support multi-byte character sets with the Communications Server SMTP (CSSMTP) application. This enhancement allows migration from SMTPD to CSSMTP for customers that use multi-byte character set code pages, and provides improved code page support for characters in the mail subject line.

To enable multi-byte character set support, complete the appropriate tasks in Table 141 on page 143.

Table 141. Task topics to enable multi-byte character set support	
Task	**Reference**
Configure CSSMTP to support multi-byte character sets. Set the MBCS statement to YES and set the TRANSLATE and MBCharset statements to multi-byte code pages.	Communications Server SMTP application in z/OS Communications Server: IP Configuration Reference
Display the values for the MBCS and MBCharset statements.	MODIFY command: Communications Server SMTP application (CSSMTP) in z/OS Communications Server: IP System Administrator's Commands

Using code page enhancements for CSSMTP

To find all related topics about code page enhancements for CSSMTP, see Table 142 on page 143.

Table 142. All related topics about code page enhancements for CSSMTP	
Book name	**Topics**
IP Configuration Guide	• Steps for creating mail on the JES spool data set for CSSMTP
IP Configuration Reference	• Communications Server SMTP application – CSSMTP configuration statements - MBCS statement - TargetServer statement - TRANSLATE statement
IP Diagnosis Guide	• Bad character translations
z/OS Communications Server: IP Programmer's Guide and Reference	• CSSMTP configuration record (CONFIG subtype 48)
IP System Administrator's Commands	• MODIFY command: Communications Server SMTP application (CSSMTP)

Chapter 6. Communications Server interface changes for z/OS V2R4

This topic the Communications Server interface changes for z/OS V2R4.

In addition to the interface changes included in this topic, refer to the following topics in the z/OS V2R4 Release Upgrade Reference Summary for additional information.

- *New and changed members in SYS1.MACLIB for z/OS V2R4*
- *New and changed SYS1.PARMLIB members for z/OS V2R4*
- *New and changed System Management Facilities (SMF) records for z/OS V2R4*

The Communications Server interface changes described in this topic are:

- "Communications Server IP interface changes" on page 145
- "Communications Server SNA interface changes" on page 168

The tables in this topic contain a **Reason for change** column that provides the name of the related functional enhancement.

Communications Server IP interface changes

This topic describes the following Communications Server IP interfaces:

- "Application programming interfaces and network management interfaces" on page 160
  - "FTP client API FCAI control block" on page 161
  - "FTP client API for REXX predefined variables" on page 161
  - "Local IPSec NMI" on page 161
  - "Network security services NMI" on page 161
  - "Real-time application-controlled TCP/IP trace NMI (EZBRCIFR)" on page 161
  - "Real-time network monitoring TCP/IP NMI" on page 161
  - "Resolver callable NMI (EZBREIFR)" on page 161
  - "SNMP manager API" on page 162
  - "Syslog daemon name/token pair" on page 162
  - "TCP/IP callable NMI (EZBNMIFR)" on page 162
  - "Trace formatting NMI (EZBCTAPI)" on page 164
  - "Trusted TCP connections API for Java" on page 164
- *Environment variables*
- *Socket APIs*
  - *General updates of socket APIs*
- *IPCS subcommands*
  - *CTRACE COMP(SYSTCPDA) subcommand*
  - *CTRACE COMP(SYSTCPIS) subcommand*
  - *CTRACE COMP(SYSTCPOT) subcommand*
  - *CTRACE COMP(SYSTCPRE) subcommand*
  - *TCPIPCS subcommand*
  - *General updates to IPCS subcommands*
- *SNMP MIB modules*
- *User exits*
- *Application data*
- *FTP client error codes*
- *SMF record type 119 enhancements*
- *z/OS UNIX /etc files*
- *General updates of IP interfaces*
- *Samples provided in MVS data set SEZAINST*
- *Samples provided in z/OS UNIX TCPIP directory*

PROFILE.TCPIP configuration file

This topic contains the PROFILE.TCPIP statement and parameter changes. The TN3270E Telnet server profile statements are accepted but ignored by the TCP/IP stack. The statements must be specified in a data set configured to the TN3270E Telnet server running in its own address space. Therefore, the Telnet configuration statements are moved from this PROFILE.TCPIP configuration file topic to a general IP configuration file topic: see "TN3270E Telnet server PROFILE configuration file" on page 148.

PROFILE.TCPIP statement and parameter changes

Table 143 on page 147 lists the new and updated Communications Server PROFILE.TCPIP configuration statements and parameters. See z/OS Communications Server: IP Configuration Reference for more detailed information.

Table 143. New and changed Communications Server PROFILE.TCPIP configuration statements and parameters for z/OS V2R4

Statement	Description	Reason for change
GLOBALCONFIG	The following new subparameter is added to the SMCGLOBAL parameter: • SMCEID/ENDSMCEID The following new subparameter is added to the SMCD parameter: • SYSTEMEID/NOSYSTEMEID	Shared Memory Communications multiple IP subnet support (SMCv2)
GLOBALCONFIG	The following new subparameters are added to the SYSPLEXMONITOR parameter: • DELAYJOINIPSEC • MONIPSEC	Sysplex Autonomics for IPSec
GLOBALCONFIG	The AUTOIQDC parameter is defined to enable and configure the HiperSockets Converged Interface function. The AUTOIQDC parameter includes the ALLTRAFFIC and NOLARGEDATA sub-parameters. The NOAUTOIQDC parameter is defined to disable the HiperSockets Converged Interface function.	HiperSockets Converged Interface support
GLOBALCONFIG	ZERT AGGREGATION INTVAL SYNCVAL • INTVAL is the recording interval that would permit a minimum of 1 hour to a maximum of 24 hours (1 day). The default setting is SMF and this indicates the zERT Aggregation interval is determined by the SMF interval. • SYNCVAL indicates a reference time for which zERT Aggregation records will begin to record. It is in the 24 hour clock format hh:mm (hour and minute value separated by a colon) and the default value is midnight or 00:00.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
GLOBALCONFIG	New subparameters AGGREGATION and NOAGGREGATION are defined on the GLOBALCONFIG ZERT parameter	z/OS Encryption Readiness Technology (zERT) aggregation
NETMONITOR	New subparameters ZERTSUMMARY and NOZERTSUMMARY are added to control the real-time zERT Summary SMF NMI service (SYSTCPES).	z/OS Encryption Readiness Technology (zERT) aggregation
SMFCONFIG	New subparameters ZERTSUMMARY and NOZERTSUMMARY are defined as TYPE119 values.	z/OS Encryption Readiness Technology (zERT) aggregation
VIPARANGE	The ZCX parameter is defined for the VIPADYNAMIC VIPARANGE statement. This indicates that Dynamic VIPAs created within this VIPARANGE are to be reserved for use by the zCX function.	Network support for z/OS Container Extensions

Configuration files

This topic includes information about the following configuration statements and files:

- “FTP client configuration statements” on page 148
- “FTP server configuration statements” on page 148
- “TN3270E Telnet server PROFILE configuration file” on page 148
- “General updates for the non-PROFILE.TCPIP IP configuration files” on page 149

The Communications Server PROFILE.TCPIP configuration file updates are in a separate topic; see “PROFILE.TCPIP configuration file” on page 146.

See z/OS Communications Server: IP Configuration Reference for more detailed information about all of the Communications Server IP configuration files and statements.

FTP client configuration statements

There is no new and changed FTP client configuration statement for V2R4.

FTP server configuration statements

There is no new or changed FTP server configuration statement in z/OS V2R4.

TN3270E Telnet server PROFILE configuration file

During initialization of the TN3270E Telnet server (Telnet) address space, configuration parameters are read from a configuration PROFILE data set. The PROFILE data set is used to configure Telnet to accept or reject connection requests. You can update the PROFILE data set to change or add statements to support new functions, or to change or add usage rules.

This topic includes tables with the descriptions of the new and changed Telnet PROFILE configuration statements. See z/OS Communications Server: IP Configuration Reference for complete information on configuration statements and the PROFILE statement.

BEGINVTAM information block

There is no new and changed BEGINVTAM information block for V2R4.

TELNETGLOBALS information block

The TELNETGLOBALS information block is a Telnet configuration block used to provide definitions that apply to all Telnet ports.

Table 144. Summary of new and changed Communications Server Telnet configuration file - TELNETGLOBALS block for z/OS V2R4

Statement	Description	Reason for change
EXPRESSLOGONMFA statement	Allows a user at a workstation, with a TELNET client and a X.509 certificate to log on to an SNA application without entering the user ID or password.	TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication

TELNETPARMS information block

Table 145. Summary of new and changed Communications Server Telnet configuration file - TELNETPARMS block for z/OS V2R4		
Statement	**Description**	**Reason for change**
EXPRESSLOGONMFA statement	Allows a user at a workstation, with a TELNET client and a X.509 certificate to log on to an SNA application without entering the user ID or password.	TN3270E Telnet server Express Logon Feature support for Multi-Factor Authentication

General updates for the non-PROFILE.TCPIP IP configuration files

Table 146 on page 149 lists the general updates for the Communications Server IP configuration files.

Table 146. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R4			
File	**Statement / Entry**	**Description**	**Reason for change**
Communications Server SMTP (CSSMTP) configuration file	ReportMailFrom	ReportMailFrom is an optional parameter that specifies the mailbox to use in the Mail From field in error reports.	SMTPD compatibility enhancements for CSSMTP (APAR PH18237)
	ReportSysoutClass	The ReportSysoutClass is an optional parameter that specifies the SYSOUT class used for error reports.	SMTPD compatibility enhancements for CSSMTP (APAR PH18237)
	MailBoxCompatibility	The MailBoxCompatibility is an optional parameter to state the size of the mail box (Standard 64 characters or Long 256 characters).	SMTPD compatibility enhancements for CSSMTP (APAR PH18237)
	MBCS TargetServer: MBCharset	• The MBCS statement is used to specify whether or not CSSMTP supports multi-byte character sets. • The multi-byte code page used by the target server to translate mail messages.	• Code page enhancements for CSSMTP

Table 146. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R4 (continued)

File	Statement / Entry	Description	Reason for change
AT-TLS policy file	New TLSv1.3 and MiddleBoxCompatMode parameters on the existing TTLSEnvironmentAdvancedParms statement.	New AT-TLS parameters and parameter values are added to AT-TLS to support TLSv1.3.	AT-TLS support for TLS v1.3
	New TLSv1.3 parameter on the existing TTLSConnectionAdvancedParms statement.		
	New cipher values for the existing V3CipherSuites4Char parameter on the TTLSCipherParms statement. New TLSv1.3 cipher values are: • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256		
	New signature algorithm pairs for the existing SignaturePairs parameter on the TTLSSignatureParms. New signature pair algorithms are: • TLS_SIGALG_SHA256_WITH_RSASSA_PSS • TLS_SIGALG_SHA384_WITH_RSASSA_PSS • TLS_SIGALG_SHA512_WITH_RSASSA_PSS		
	New ECDH (Elliptic curve Diffie-Hellman) curves for the existing ClientECurves parameter on the TTLSSignatureParms. New curves are: • x25519 • x448		

Table 146. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R4 (continued)

File	Statement / Entry	Description	Reason for change
AT-TLS policy file	New parameters ClientKeyShareGroups, ServerKeyShareGroups, and SignaturePairsCert on the existing TTLSSignatureParms statement.	New AT-TLS parameters and parameter values are added to AT-TLS to support TLSv1.3.	AT-TLS support for TLS v1.3
	Default values added for the existing ClientECurves and SignaturePairs parameters on the TTLSSignatureParms statement. The policy agent default value for ClientECurves is equivalent to the existing System SSL default value. The policy agent default value for SignaturePairs is equivalent to the existing System SSL default, with the new RSASSA_PSS values included at the end.		
	New signature algorithm pairs for the existing OcspRequestSigAlg and OcspResponseSigAlgPairs parameters on the TTLSGskOcspParms statement. New signature pair algorithms are: • TLS_SIGALG_SHA256_WITH_RSASSA_PSS • TLS_SIGALG_SHA384_WITH_RSASSA_PSS • TLS_SIGALG_SHA512_WITH_RSASSA_PSS		

Table 146. New and changed non-PROFILE.TCPIP configuration files for z/OS V2R4 (continued)			
File	**Statement / Entry**	**Description**	**Reason for change**
AT-TLS policy file	New parameters on the existing TTLSGskAdvancedParms statement. The new parameters are: • GSK_SESSION_TICKET_CLIENT_ENABLE • GSK_SESSION_TICKET_CLIENT_MAXSIZE • GSK_SESSION_TICKET_SERVER_ALGORITHM • GSK_SESSION_TICKET_SERVER_COUNT • GSK_SESSION_TICKET_SERVER_ENABLE • GSK_SESSION_TICKET_SERVER_TIMEOUT • GSK_SESSION_TICKET_SERVER_KEY_REFRESH	New AT-TLS parameters and parameter values are added to AT-TLS to support TLSv1.3.	AT-TLS support for TLS v1.3
	Default values added for the existing GSK_V3_SESSION_TIMEOUT and GSK_V3SIDCACHE_SIZE parameters on the TTLSGskAdvancedParms statement. The policy agent defaults are equivalent to the existing System SSL default values.		
IKE daemon configuration file	New parameter NoKeyRing on the existing IkeConfig statement	NoKeyRing can be specified when no IKED key ring is provided.	Sysplex Autonomics for IPSec
Resolver setup file	MAXNEGTTL	New statement that specifies the maximum amount of time that the resolver can cache negative responses from a Domain Name System (DNS) name server.	Communications server miscellaneous enhancements

RACF interfaces

Table 147 on page 153 lists the functions for which new or changed RACF support is available. Sample RACF commands to change the RACF configuration can be found in one of the following members of the installation data set, SEZAINST:

- EZARACF - Contains sample commands for environments where multilevel security is not configured.
- EZARACFM - Contains sample commands for environments where multilevel security is configured.

You can use the function name from the table to search EZARACF for all the commands necessary for the function. See z/OS Communications Server: IP Configuration Guide for more information for each function.

Table 147. New and changed Communications Server RACF interfaces for z/OS V2R4

Function name	Description	Reason for change
EZB.NETMGMT.sysname.tcpname.SYSTCPES	New SAF resource to control access to SYSTCPES real-time NMI SMF service	z/OS Encryption Readiness Technology (zERT) aggregation
EZB.FTP.*sysname.ftpdaemonname*.ACCESS.JES	New SAF resource defined in the SERVAUTH class	FTP server JES access control

Operator commands

This topic includes information about the following Communications Server IP operator commands:

- “Netstat operator commands (DISPLAY TCPIP,,NETSTAT)” on page 153
- “TN3270E Telnet server operator commands” on page 155
- “General updates of IP operator commands” on page 155

See z/OS Communications Server: IP System Administrator's Commands for more detailed information.

Netstat operator commands (DISPLAY TCPIP,,NETSTAT)

Table 148 on page 153 lists the new and updated Communications Server IP Netstat operator command DISPLAY TCPIP,,NETSTAT. See Table 150 on page 155 for the other Communications Server IP operator command entries.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server IP operator commands.

All parameters in the following table are for the DISPLAY TCPIP,,NETSTAT operator command.

Table 148. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R4

Parameters	Description	Reason for change
ALL	The following information is now displayed under the SMC INFORMATION section: • SMCDVERSION • SMCEID	Shared Memory Communications multiple IP subnet support (SMCv2)
ARP	Displays ARP information for the HiperSockets Converged Interfaces.	HiperSockets Converged Interface support
CONFIG	The configured SMCEIDs are listed in the SMCGlobal section. Whether a SMCDSYSEID is configured and its value, if configured, is displayed in the SMCD section.	Shared Memory Communications multiple IP subnet support (SMCv2)
CONFIG	The Global Configuration Information section of the display includes the new Sysplex Monitor settings - DelayJoinIpsec and MonIpsec.	Sysplex Autonomics for IPSec

Table 148. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R4 (continued)

Parameters	Description	Reason for change
CONFIG	Displays the setting of the AUTOIQDC parameter.	HiperSockets Converged Interface support
CONFIG	Displays new ZERT Aggregation sub parameter information with INTVAL and SYNCVAL in the GLOBALCONFIG section.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
CONFIG	• Displays new ZERTSUMMARY subparameter information in the SMFCONFIG section. • Displays new ZERT Aggregation subparameter information in the GLOBALCONFIG section. • Displays new ZERTSUMMARY subparameter information in the NETMONITOR section.	z/OS Encryption Readiness Technology (zERT) aggregation
DEvlinks	The card generation level and speed information are displayed for RNIC interfaces representing "RoCE Express3" features.	Communications Server support for RoCE Express3
DEvlinks	Specifying PNETID=NONE will display all SMC-D capable interfaces without a PNETID. Specifying PNETID=* will display all SMC-D capable interfaces without a PNETID under a new PNETID=*NONE* heading. Specifying an INTFNAME of an SMC-D capable interface will display any unassociated ISM interfaces. Specifying SMC will display the following information under the SMCD LINK INFORMATION section: • SMCDversion • SMCEID • Remote hostname • Remote host type	Shared Memory Communications multiple IP subnet support (SMCv2)
DEvlinks	• Displays the name of the HiperSockets Converged Interface, if any, that is associated with an OSD and statistics related to that associated interface. • Displays the name of the zCX interface, if any, and statistics related to that interface. • Displays the name of the zCX DVIPA interface, if any, and statistics related to that interface.	• HiperSockets Converged Interface support • Network support for z/OS Container Extensions • Network support for z/OS Container Extensions
ND	Displays ND information for the HiperSockets Converged Interfaces.	HiperSockets Converged Interface support

Table 148. New and changed Communications Server Netstat operator commands (DISPLAY TCPIP,,NETSTAT) for z/OS V2R4 (continued)		
Parameters	**Description**	**Reason for change**
TTLS	• The negotiated TLS protocol and cipher can have new values for TLSv1.3. • For a connection secured with TLSv1.3, the negotiated key share is displayed. • **With the DETAIL option,** new AT-TLS policy configuration parameters are displayed for a connection.	AT-TLS support for TLS v1.3
VIPADCFG	Displays the setting of the ZCX parameter on the VIPARANGE statement.	Network support for z/OS Container Extensions
VIPADYN	Indicates whether a DVIPA with an origin of VIPARANGE IOCTL was created for zCX.	Network support for z/OS Container Extensions

TN3270E Telnet server operator commands

Table 149 on page 155 includes the descriptions of the new and changed TN3270E Telnet server operator commands. Refer to *z/OS Communications Server: IP System Administrator's Commands* for complete information on Telnet operator commands.

Table 149. New and changed Communications Server TN3270E Telnet server operator commands for z/OS V2R4	
Command	**Description**
Display TCPIP,,Telnet,COnn	The ACCESS fields can display new 4-byte ciphers and can display a protocol value of TLSV1.3.

General updates of IP operator commands

Table 150 on page 155 lists the new and updated Communications Server IP operator commands, **except** the Netstat operator command DISPLAY TCPIP,,NETSTAT and the Telnet operator commands. See the following tables for those commands:

- Table 148 on page 153, IP Netstat operator commands (DISPLAY TCPIP,,NETSTAT)
- "TN3270E Telnet server operator commands" on page 155, Telnet operator commands

Table 150. New and changed Communications Server operator commands for z/OS V2R4			
Command	**Parameters**	**Description**	**Reason for change**
MODIFY	RESOLVER,REFRESH| DISPLAY	Enhanced to include the most recently used resolver setup file and the value of the MAXNEGTTL resolver setup statement.	Communications Server miscellaneous enhancements
MODIFY CSSMTP	DISPLAY,CONFIG	Display the new values for ReportMailFrom, ReportSysoutClass, and MailBoxCompatibility statements Display the new MBCS statement and MBCharset parameter on the TargetServer statement	SMTPD compatibility enhancements for CSSMTP (APAR PH18237) Code page enhancements for CSSMTP
MODIFY IKED	DISPLAY	Display includes the NoKeyRing parameter if configured.	Sysplex Autonomics for IPSec

TSO commands

This topic includes information about the following TSO commands:

- “NETSTAT TSO commands” on page 156
- “FTP TSO and z/OS UNIX commands” on page 158
- “General updates of IP operator commands” on page 155

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server TSO commands.

NETSTAT TSO commands

Table 151 on page 156 lists the new and updated Communications Server NETSTAT TSO command.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server TSO commands.

Table 151. New and changed Communications Server NETSTAT TSO commands for z/OS V2R4

Parameter	Description	Reason for change
ALL	The following information is displayed under the SMC INFORMATION section: • SMCDVERSION • SMCEID	Shared Memory Communications multiple IP subnet support (SMCv2)
ARP	Displays ARP information for the HiperSockets Converged Interfaces.	HiperSockets Converged Interface support
CONFIG	The configured SMCEIDs are listed in the SMCGlobal section. Whether a SMCDSYSEID is configured and its value, if configured, is displayed in the SMCD section.	Shared Memory Communications multiple IP subnet support (SMCv2)
CONFIG	The Global Configuration Information section of the display includes the new Sysplex Monitor settings - DelayJoinIpsec and MonIpsec.	Sysplex Autonomics for IPSec
CONFIG	Displays the setting of the AUTOIQDC parameter.	HiperSockets Converged Interface support
CONFIG	Displays new ZERT Aggregation subparameter information with INTVAL and SYNCVAL in the GLOBALCONFIG section.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
CONFIG	• Displays new ZERTSUMMARY subparameter information in the SMFCONFIG section. • Displays new ZERT aggregation subparameter information in the GLOBALCONFIG section. • Displays new ZERTSUMMARY subparameter information in the NETMONITOR section.	z/OS Encryption Readiness Technology (zERT) aggregation

Table 151. New and changed Communications Server NETSTAT TSO commands for z/OS V2R4 (continued)

Parameter	Description	Reason for change
DEvlinks	The card generation level and speed information are displayed for RNIC interfaces representing "RoCE Express3" features.	Communications Server support for RoCE Express3
DEvlinks	Specifying PNETID=NONE will display all SMC-D capable interfaces without a PNETID. Specifying PNETID=* will display all SMC-D capable interfaces without a PNETID under a new PNETID=*NONE* heading. Specifying INTFNAME of an SMC-D capable interface will display any unassociated ISM interfaces. Specifying SMC will display the following information under the SMCD LINK INFORMATION section: • SMCDversion • SMCEID • Remote hostname • Remote host type	Shared Memory Communications multiple IP subnet support (SMCv2)
DEvlinks	• Displays the name of the HiperSockets Converged Interface, if any, that is associated with an OSD and statistics related to that associated interface. • Displays the name of the zCX interface, if any, and statistics related to that interface. • Displays the name of the zCX DVIPA interface, if any, and statistics related to that interface.	• HiperSockets Converged Interface support • Network support for z/OS Container Extensions • Network support for z/OS Container Extensions
ND	Displays ND information for the HiperSockets Converged Interfaces.	HiperSockets Converged Interface support
TTLS	• The negotiated TLS protocol and cipher can have new values for TLSv1.3. • For a connection secured with TLSv1.3, the negotiated key share is displayed. • **With the DETAIL option,** new AT-TLS policy configuration parameters are displayed for a connection.	AT-TLS support for TLS v1.3
VIPADCFG	Displays the setting of the ZCX parameter on the VIPARANGE statement.	Network support for z/OS Container Extensions
VIPADYN	Indicates whether a DVIPA with an origin of VIPARANGE IOCTL was created for zCX.	Network support for z/OS Container Extensions

FTP TSO and z/OS UNIX commands

There are no new or changed FTP TSO and z/OS UNIX commands for z/OS V2R4.

FTP subcommands

There are no new or changed FTP subcommands for z/OS V2R4.

General updates of TSO commands

There are no general updates of TSO commands for z/OS V2R4.

z/OS UNIX commands

"General updates of z/OS UNIX commands" on page 160 lists the new and updated z/OS UNIX commands, except the z/OS UNIX FTP commands, and the z/OS UNIX netstat commands. See the following tables for those commands:

- "FTP subcommands" on page 158, FTP TSO and z/OS UNIX commands
- Table 152 on page 158, z/OS UNIX netstat commands

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the Communications Server UNIX commands.

Netstat UNIX commands

Table 152 on page 158 lists the new and updated Communications Server z/OS UNIX netstat command. See "General updates of z/OS UNIX commands" on page 160 for the other (the non-netstat) z/OS UNIX command entries.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the z/OS UNIX commands.

All parameters in the following table are for the z/OS UNIX netstat command.

Table 152. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R4

Parameter	Description	Reason for change
-A	The following information is displayed under the SMC INFORMATION section: • SMCDVERSION • SMCEID	Shared Memory Communications multiple IP subnet support (SMCv2)
-d	The card generation level and speed information are displayed for RNIC interfaces representing "RoCE Express3" features.	Communications Server support for RoCE Express3

Table 152. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R4 (continued)

Parameter	Description	Reason for change
-d	Specifying PNETID=NONE will display all SMC-D capable interfaces without a PNETID. Specifying PNETID=* will display all SMC-D capable interfaces without a PNETID under a new PNETID=*NONE* heading. Specifying INTFNAME of an SMC-D capable interface will display any unassociated ISM interfaces. Specifying SMC will display the following information under the SMCD LINK INFORMATION section: • SMCDversion • SMCEID • Remote hostname • Remote host type	Shared Memory Communications multiple IP subnet support (SMCv2)
-d	Displays the name of the HiperSockets Converged Interface, if any, that is associated with an OSD and statistics related to that associated interface.	HiperSockets Converged Interface support
-d	• Displays the name of the zCX interface, if any, and statistics related to that interface. • Displays the name of the zCX DVIPA interface, if any, and statistics related to that interface.	• Network support for z/OS Container Extensions • Network support for z/OS Container Extensions
-F	Displays the setting of the ZCX parameter on the VIPARANGE statement.	Network support for z/OS Container Extensions
-f	The configured SMCEIDs are listed in the SMCGlobal section. Whether a SMCDSYSEID is configured and its value, if configured, is displayed in the SMCD section.	Shared Memory Communications multiple IP subnet support (SMCv2)
-f	The Global Configuration Information section of the display includes the new Sysplex Monitor settings - DelayJoinIpsec and MonIpsec.	Sysplex Autonomics for IPSec
-f	Displays the setting of the AUTOIQDC parameter.	HiperSockets Converged Interface support
-f	Displays new ZERT Aggregation sub parameter information with INTVAL and SYNCVAL in the GLOBALCONFIG section.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval

Table 152. New and changed Communications Server z/OS UNIX netstat commands for z/OS V2R4 (continued)		
Parameter	**Description**	**Reason for change**
-f	• Displays new ZERTSUMMARY subparameter information in the SMFCONFIG section. • Displays new ZERT Aggregation subparameter information in the GLOBALCONFIG section. • Displays new ZERTSUMMARY subparameter information in the NETMONITOR section.	z/OS Encryption Readiness Technology (zERT) aggregation
-n	Displays ND information for the HiperSockets Converged Interfaces.	HiperSockets Converged Interface support
-R	Displays ARP information for the HiperSockets Converged Interfaces.	HiperSockets Converged Interface support
-x	• The negotiated TLS protocol and cipher can have new values for TLSv1.3. • For a connection secured with TLSv1.3, the negotiated key share is displayed. • **With the DETAIL option,** new AT-TLS policy configuration parameters are displayed for a connection.	AT-TLS support for TLS v1.3
-v	Indicates whether a DVIPA with an origin of VIPARANGE IOCTL was created for zCX.	Network support for z/OS Container Extensions

General updates of z/OS UNIX commands

Table 153 on page 160 lists the new and updated Communications Server z/OS UNIX non-netstat command.

See z/OS Communications Server: IP System Administrator's Commands for more detailed information about the z/OS UNIX commands.

All parameters in the following table are for the z/OS UNIX non-netstat command.

Table 153. New and changed Communications Server z/OS UNIX commands for z/OS V2R4			
Command	**Parm**	**Description**	**Reason for change**
pasearch	N/A	New AT-TLS policy configuration parameters are displayed.	AT-TLS support for TLS v1.3

Application programming interfaces and network management interfaces

This topic includes updates made to the application programming interfaces (APIs) and network management interfaces (NMIs) documented in z/OS Communications Server: IP Programmer's Guide and Reference. The following programming interfaces were updated:

- “FTP client API FCAI control block” on page 161
- “FTP client API for REXX predefined variables” on page 161
- “Local IPSec NMI” on page 161

- “Network security services NMI” on page 161
- “Real-time application-controlled TCP/IP trace NMI (EZBRCIFR)” on page 161
- “Real-time network monitoring TCP/IP NMI” on page 161
- “Resolver callable NMI (EZBREIFR)” on page 161
- “SNMP manager API” on page 162
- “Syslog daemon name/token pair” on page 162
- “TCP/IP callable NMI (EZBNMIFR)” on page 162
- “Trace formatting NMI (EZBCTAPI)” on page 164
- “Trusted TCP connections API for Java” on page 164

See z/OS Communications Server: IP Programmer's Guide and Reference for more detailed API information.

FTP client API FCAI control block

There are no new or changed FTP client API FCAI control block for z/OS V2R4.

FTP client API for REXX predefined variables

There are no new or changed FTP client API for REXX predefined variables for z/OS V2R4.

Local IPSec NMI

There are no new or changed Local IPSec NMI for z/OS V2R4.

Network security services NMI

There are no new or changed Network security services NMI for z/OS V2R4.

Real-time application-controlled TCP/IP trace NMI (EZBRCIFR)

There are no new or changed Real-time application-controlled TCP/IP trace NMI (EZBRCIFR) for z/OS V2R4.

Real-time network monitoring TCP/IP NMI

There is no new or changed real-time network monitoring TCP/IP NMI for z/OS V2R4.

Table 154 on page 161 lists the updates to the Communications Server real-time TCP/IP network monitoring NMI. For changes to SMF 119 records provided by the real-time SMF data NMI (SYSTCPSM) and the real-time TCP connection SMF data NMI (SYSTCPCN), see “SMF record type 119 enhancements” on page 167.

Table 154. New Communications Server real-time TCP/IP NMI for z/OS V2R4

NMI	Request/response	Description	Reason for change
Real-time zERT Summary SMF NMI (SYSTCPES)	zERT summary record (subtype 12)	New real-time SMF service for zERT summary data	z/OS Encryption Readiness Technology (zERT) aggregation

Resolver callable NMI (EZBREIFR)

There are no new or changed Resolver callable NMI (EZBREIFR) for z/OS V2R4.

Table 155 on page 162 lists the new and changed resolver callable NMI (EZBREIFR) for z/OS V2R4.

Table 155. New Communications Server resolver callable NMI (EZBREIFR) for z/OS V2R4	
Request	**Description**
GetResolverConfig	Added the following information: • NMSSOptions(NMSSOMaxNegTTL), a new flag to indicate that the MAXNEGTTL function is active • NMSSDefaults(NMSSDMaxNegTTL), a new flag to indicate that the MAXNEGTTL value was defaulted • NMSSetupMaxNegTTL, a new field to contain the MAXNEGTTL value, in seconds

SNMP manager API

There are no new or changed SNMP manager API for z/OS V2R4.

Syslog daemon name/token pair

There are no new or changed syslog daemon name/token pair for z/OS V2R4

TCP/IP callable NMI (EZBNMIFR)

Table 156 on page 162 lists the updates to the Communications Server TCP/IP callable NMI.

Table 156. New Communications Server TCP/IP callable NMI (EZBNMIFR) for z/OS V2R4			
Request	**Parameter/output**	**Description**	**Reason for change**
GetConnectionDetail	• NWMConnSMCVersion • NWMConnSMCEID	These new fields indicate the SMC characteristics of the connection.	Shared Memory Communications multiple IP subnet support (SMCv2)
GetConnectionDetail	• NWMConnTTLSSSLProt • NWMConnTTLSNegCiph4 • NWMConnTTLSKeyShare	AT-TLS support for TLS v1.3 • NWMConnTTLSSSLProt (negotiated TLS protocol) can have a new value of x'0304' for TLSv1.3 • NWMConnTTLSNegCiph4 (negotiated 4-byte cipher) can have new values • NWMConnTTLSKeyShare (negotiated TLSv1.3 key share) – new field	AT-TLS support for TLS v1.3
GetDVIPAList	NWMDvListFlags	A new flag, NWMDVListFlags_DVRZCX (0x02), is added. The flag means that an application instance DVIPA was created for zCX. These DVIPAs are created within the range defined by a VIPARANGE statement with the ZCX keyword.	Network support for z/OS Container Extensions
GetIfs	• NWMIfSMCRStatus • NWMIfSMCDStatus	• – The following values are obsolete from the NWMIfSMCRStatus field: - NWMIFSMCRNOPNETID - NWMIFSMCRNOGC - NWMIFSMCRNOSUBMSK • – The following values are obsolete from the NWMIfSMCDStatus field: - NWMIFSMCDNOPNETID - NWMIFSMCDNOGC - NWMIFSMCDNOSUBMSK - NWMIFSMCDPNETIDMISCFG	Shared Memory Communications multiple IP subnet support (SMCv2)
GetIfs	NWMIfType • NWMIFTZCX	There is a new value for NWMIfType (NWMIFTZCX). This new value indicates that the interface being displayed is a zCX Interface.	Network support for z/OS Container Extensions

Table 156. New Communications Server TCP/IP callable NMI (EZBNMIFR) for z/OS V2R4 (continued)

Request	Parameter/output	Description	Reason for change
GetIfs	• NWMIfFlags2 – NWMIFIQDCFLG • NWMIfIQDCName • NWMIfType – NWMIFTHIPERIQDC	• New flag bit NWMIFIQDCFLG indicates that NWMIfIQDCName contains the name of the associated HiperSockets IQDC Interface. • NWMIfIQDCName contains the name of associated HiperSockets IQDC interface. • There is a new value for NWMIfType (NWMIFTHIPERIQDC). This new value indicates that the interface being displayed is a HiperSockets Converged Interface.	HiperSockets Converged Interface support
GetIfStats	NWMIfStType • NWMIFTZCX	There is a new value for NWMIfStType (NWMIFTZCX). This new value indicates that the interface being displayed is a zCX Interface.	Network support for z/OS Container Extensions
GetIfStats	• NWMIfStFlags – NWMIFSTIQDCFLG • NWMIfStType – NWMIFTHIPERIQDC • NWMIfStInIQDCBytes • NWMIfStInIQDCUcastPkts • NWMIfStOutIQDCBytes • NWMIfStOutIQDCUcastPkts	• New flag bit NWMIFSTIQDCFLG indicates that statistics for the associated HiperSockets IQDC interface are provided in NWMIfStIQDXStats area of this record. • There is a new value for NWMIfStType (NWMIFTHIPERIQDC). This new value indicates that the interface being displayed is a HiperSockets Converged Interface. • Input bytes received over associated HiperSockets IQDC interface. • Input unicast packets received over associated HiperSockets IQDC interface. • Output bytes sent over associated HiperSockets IQDC interface. • Output unicast packets sent over associated HiperSockets IQDC interface.	HiperSockets Converged Interface support
GetIfStatsExtended	NWMIfStExtIType • NWMIFTHIPERIQDC	There is a new value for NWMIfStExtIType (NWMIFTHIPERIQDC). This new value indicates that the interface being displayed is a HiperSockets Converged Interface.	HiperSockets Converged Interface support
GetProfile	• NMTP_GBCFSYSTEMEID • NMTP_GBCFSYSTEMEIDSTR • NMTP_GBCFSMCEID • NMTP_GBCFSMCEIDCount • NMTP_GBCFUEIDList	These new fields indicate the settings of the new GLOBALCONFIG parameters.	Shared Memory Communications multiple IP subnet support (SMCv2)
GetProfile	NMTP_GBCFAUTOIQDC	New byte NMTP_GBCFAUTOIQDC indicates the setting of AUTOIQDC in the GLOBALCONFIG statement.	HiperSockets Converged Interface support
GetProfile	Global configuration section: • NMTP_GBCFZERTINTV • NMTP_GBCFZERTSYNC	• New NMTP_GBCFZERTINTV flag bit that indicates the setting of the INTVAL sub-parameter on the GLOBALCONFIG statement. • New NMTP_GBCFZERTSYNC flag bit that indicates the setting of the SYNCVAL sub-parameter on the GLOBALCONFIG statement.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
GetProfile	Management section: • NMTP_MGMTSmf119Types • NMTP_MGMT119ZertSummary • NMTP_MGMTNetMonServices • NMTP_MGMTNMZertSummary	• New NMTP_MGMT119ZertSummary flag bit is set in the NMTP_MGMTSmf119Types field to indicate that the new zERT summary record was requested on the SMFCONFIG TYPE119 profile statement. • NMTP_MGMTNMZertSummary flag bit is set in the NMTP_MGMTNetMonServices field to indicate that the new zERT summary records were requested on the NETMONITOR profile statement.	z/OS Encryption Readiness Technology (zERT) aggregation
GetProfile	Global configuration section: • NMTP_GBCFSysMonDelayJoinI • NMTP_GBCFSysMonIpsec	New fields, NMTP_GBCFSysMonDelayJoinI and NMTP_GBCFSysMonIpsec, indicate the settings of the new SYSPLEXMONITOR subparameters	Sysplex Autonomics for IPSec
GetRnics	NWMRnicBGen	Value of NWMRNICBGENREXP3 represents the RoCE Express3 feature.	Communications Server support for RoCE Express3

Table 156. New Communications Server TCP/IP callable NMI (EZBNMIFR) for z/OS V2R4 (continued)			
Request	**Parameter/output**	**Description**	**Reason for change**
GetSmcDLinks	• NWMSmcDLnkSMCEID • NWMSmcDLnkVersion • NWMSmcDLnkRemoteOSType • NWMSmcDLnkRmtHostName	These new fields indicate the SMC characteristics of the SMCD link.	Shared Memory Communications multiple IP subnet support (SMCv2)
GetStorageStatistics	• NWMStgFlags – NWMStgZAGGCfg • New ZERT aggregation storage utilization fields – NWMStg64ZaggCurrent – NWMStg64ZaggMax	• New flag bit NWMStgZaggCfg indicates whether ZERT AGGREGATION is configured on the GLOBALCONFIG statement. • New fields NWMStg64ZaggCurrent and NWMStg64ZaggMax provide current and maximum storage usage statistics for ZERT AGGREGATION.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval

Trace formatting NMI (EZBCTAPI)

There are no new or changed trace formatting NMI (EZBCTAPI) for z/OS V2R4.

Trusted TCP connections API for Java

There are no new or changed trusted TCP connections API for Java for z/OS V2R4.

Environment variables

There are no new or changed environment variables for z/OS V2R4.

Socket APIs

This topic includes information about Communications Server socket APIs.

Refer to the following documents for more information about socket APIs:

- For complete documentation of the z/OS UNIX C sockets APIs, refer to z/OS XL C/C++ Runtime Library Reference
- For information about z/OS UNIX Assembler Callable Services, refer to z/OS UNIX System Services Programming: Assembler Callable Services Reference
- For information about TCP/IP socket APIs, refer to z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference
- For information about TCP/IP CICS sockets, refer to z/OS Communications Server: IP CICS Sockets Guide

General updates of socket APIs

Table 157 on page 165 lists the general updates made to the IP socket APIs.

Table 157. New and changed Communications Server socket APIs for z/OS V2R4			
Socket API	**Function call/Parameter**	**Description**	**Reason for change**
• **Call instruction** • **CICS® C** • **CICS sockets extended** • **MACRO** • **REXX socket** • **UNIX assembler callable services** • **XL C/C++**	SIOCTTLSCTL ioctl	• TTLSi_SSL_Protocol updated to support TLSv1.3 • TTLSi_Neg_Cipher4 updated to support new cipher values • TTLSi_Neg_KeyShare – new field that contains the negotiated TLSv1.3 key share • TTLSi_Req_Type – New request options TTLS_RESET_WRITE_CIPHER and TTLS_SEND_SESSION_TICKET are provided	AT-TLS support for TLS v1.3

IPCS subcommands

This topic includes information about these IPCS subcommands:

See z/OS Communications Server: IP Diagnosis Guide for more detailed IPCS subcommands information.

CTRACE COMP(SYSTCPDA) subcommand

This topic lists changes to Communications Server CTRACE COMP(SYSTCPDA) subcommand options for z/OS V2R4.

There are no new or changed CTRACE COMP(SYSTCPDA) subcommand for z/OS V2R4.

CTRACE COMP(SYSTCPIS) subcommand

This topic describes the Communications Server CTRACE COMP(SYSTCPIS) subcommand options for z/OS V2R4.

There are no new or changed CTRACE COMP(SYSTCPIS) subcommand for z/OS V2R4.

CTRACE COMP(SYSTCPOT) subcommand

This topic lists changes to Communications Server CTRACE COMP(SYSTCPDA) subcommand options for z/OS V2R4.

There are no new or changed CTRACE COMP(SYSTCPOT) subcommand for z/OS V2R4.

CTRACE COMP(SYSTCPRE) subcommand

This topic describes the CTRACE COMP(SYSTCPRE) subcommand options for z/OS V2R4.

There are no new or changed CTRACE COMP(SYSTCPRE) subcommand for z/OS V2R4.

TCPIPCS subcommand

This topic describes the Communications Server TCPIPCS subcommand option changes for z/OS V2R4.

Table 158 on page 166 lists the TCPIPCS subcommand options.

The TCPIPCS command contains the OPTLOCAL specification in some displays.

Table 158. New and changed Communications Server TCPIPCS subcommand options for z/OS V2R4

Subcommand	Description	Reason for change
CONFIG	The unassociated ISM interfaces will be displayed.	Shared Memory Communications multiple IP subnet support (SMCv2)
CONFIG	• Includes the new HiperSockets Converged Interfaces in the output. • Includes the new zCX interface in the output.	• HiperSockets Converged Interface support • Network support for z/OS Container Extensions
PROFILE	Displays the new INTVAL and SYNCVAL sub-parameters for the GLOBALCONFIG statement.	z/OS Encryption Readiness Technology (zERT) aggregation recording interval
PROFILE	The configured SMCEIDs and the SYSTEMEID will be displayed.	Shared Memory Communications multiple IP subnet support (SMCv2)
PROFILE	The display includes the new Sysplex Monitor subparameters – DELAYJOINIPSEC and MONIPSEC.	Sysplex Autonomics for IPSec
PROFILE	• Displays the AUTOIQDC parameter. • Displays the new ZCX parameter for VIPARANGE.	• HiperSockets Converged Interface support • Network support for z/OS Container Extensions
STATE	The report includes a new table, the IKED Heartbeat Historical Data table	Sysplex Autonomics for IPSec
STATE	Includes the new HiperSockets Converged Interfaces in the output.	HiperSockets Converged Interface support
TREE	Includes the new HiperSockets Converged Interfaces in the output.	HiperSockets Converged Interface support
TTLS	Updated to display new AT-TLS parameters and values.	AT-TLS support for TLS v1.3

General updates to IPCS subcommands

There are no new or changed general updates to IPCS subcommands for z/OS V2R4.

SNMP MIB modules

This topic lists updates to Communications Server's support for SNMP MIB modules.

For a complete list of supported SNMP MIB objects, refer to z/OS Communications Server: IP System Administrator's Commands.

Table 159 on page 167 lists the changes to the SNMP MIB module support.

Table 159. New and changed Communications Server SNMP MIB module support for z/OS V2R4

MIB module name	Description	Reason for change
IBMTCPIPMVS-MIB	• The ibmMvsIfType MIB object supports a new value, ipaqiqdc(41), to indicate an entry in the table is an IPAQIQDC interface. • The ibmMvsIfType MIB object supports a new value, ipaqiqdc6(42), to indicate an entry in the table is an IPAQIQDC6 interface. • The ibmMvsIfTrleName MIB object is supported for OSD, OSX, IPAQIQDC, and IPAQIQDC6 interfaces. • The ibmMvsIfPNetID MIB object is supported for IPAQIQDC and IPAQIQDC6 interfaces.	HiperSockets Converged Interface support
IBMTCPIPMVS-MIB	The ibmMvsTcpConnectionTtlsSslProt MIB object supports a new value, tlsVer1Dot3(7), to indicate TLS protocol Version 1.3.	AT-TLS support for TLS v1.3

User exits

There are no new or changed user exits for z/OS V2R4.

Application data

There are no new or changed application data for z/OS V2R4.

FTP client error codes

This topic describes new client error codes for the FTP client.

There are no new or changed FTP client error codes for z/OS V2R4.

SMF record type 119 enhancements

See New and changed System Management Facilities (SMF) records for z/OS V2R4 in z/OS Release Upgrade Reference Summary for information on new and changed SMF type 119 records.

See the Type 119 SMF records topic in z/OS Communications Server: IP Programmer's Guide and Reference for more information.

z/OS UNIX /etc files

Changes to z/OS UNIX /etc files are listed in *IP Services: Update /etc configuration files* in z/OS Upgrade Workflow.

General updates of IP interfaces

There are no general updates of IP interface for z/OS V2R4.

Samples provided in MVS data set SEZAINST

Table 160 on page 168 lists the changes to the samples that are provided in MVS data set SEZAINST.

Table 160. IP samples provided in MVS data set SEZAINST for z/OS V2R4

Member	Description	Reason for change
CSSMTPCF	This CSSMTP sample configuration file is updated to add information about ReportMailFrom, ReportSysoutClass, and MailBoxCompatibility. This CSSMTP sample configuration file is updated to add information about MBCS and MBCharset.	SMTPD compatibility enhancements for CSSMTP (APAR PH18237) Code page enhancements for CSSMTP
EZARACF	A new resource profile in the SERVAUTH class is provided for the EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES resource	FTP server JES access control
RESSETUP	Includes a description of the new MAXNEGTTL resolver setup statement.	Communications Server miscellaneous enhancements

Samples provided in z/OS UNIX TCPIP directory

Table 161 on page 168 lists the changes to the samples that are provided in z/OS UNIX directory /usr/lpp/tcpip/samples.

Table 161. IP samples provided in z/OS UNIX directory /usr/lpp/tcpip/samples for z/OS V2R4

File name	Description
EZAIKCFG	The IKE configuration file sample has been updated to add the NoKeyRing parameter.

Communications Server SNA interface changes

This topic describes the following Communications Server SNA interfaces:

Start options

Table 162 on page 169 lists the new or changed SNA start options.

Refer to *z/OS Communications Server: SNA Resource Definition Reference* for more information on start options.

Table 162. New and changed Communications Server start options for z/OS V2R4		
Start option	**Description of update**	**Reason for change**
INOPDUMP	ZCX has been added as new control group (ctrlgrp) value.	Network support for z/OS Container Extensions
QDIOEIB	When set to ENABLED, specifies whether VTAM will enable the Enhanced Inbound Block (EIB) function within the OSA-Express feature for all eligible QDIO interfaces for all TCP/IP stacks.	OSA-Express Enhanced Inbound Blocking (EIB)

Start option behavior changes

There are no start option behavior changes for z/OS V2R4.

Definition statements

There are no new or changed definition statements for z/OS V2R4.

Commands

Table 163 on page 169 lists the new and changed SNA commands.

For complete information about SNA commands, refer to the *z/OS Communications Server: SNA Operation*.

Table 163. New and changed Communications Server commands in z/OS V2R4		
Command	**Description**	**Reason for change**
DISPLAY NET,TRL	The value ZCX was added as a new CONTROL operand.	Network support for z/OS Container Extensions

Command behavior changes

Table 164 on page 169 lists the SNA commands that have changed behavior.

For complete information about SNA commands, refer to the *z/OS Communications Server: SNA Operation*.

Table 164. New and changed Communications Server commands with changed behavior for z/OS V2R4		
Command	**Description of behavior change**	**Reason for change**
DISPLAY ID	• If the resource that is being displayed is a RDMA over Converged Ethernet (RoCE) TRLE, message IST2389I contains the "RoCE Express" generation level and the transmission speed. RoCE Express3 was added to the RoCE Express generation level. • If the resource that is being displayed is a RoCE Express3 TRLE, message IST2362I always displays the microcode level.	Communications Server support for RoCE Express3

Table 164. New and changed Communications Server commands with changed behavior for z/OS V2R4 (continued)		
Command	**Description of behavior change**	**Reason for change**
DISPLAY TRL	• If the TRLE operand specifies a RDMA over Converged Ethernet (RoCE) TRLE, message IST2389I contains the "RoCE Express" generation level and the transmission speed. RoCE Express3 was added to the RoCE Express generation level. • If the TRLE operand specifies a RoCE Express3 TRLE, message IST2362I always displays the microcode level.	Communications Server support for RoCE Express3
DISPLAY NET,ID	zCX TRLEs displayed by the D NET,ID command will indicate CONTROL=ZCX.	Network support for z/OS Container Extensions
DISPLAY NET,TRL	zCX TRLEs displayed by the D NET,TRL command will indicate CONTROL=ZCX.	Network support for z/OS Container Extensions
DISPLAY NET,ID=*trlename*	QDIO TRLEs will display additional information if there have been any read errors.	Communications Server miscellaneous enhancements
DISPLAY NET,TRL,TRLE=*trlename*	QDIO TRLEs will display additional information if there have been any read errors.	Communications Server miscellaneous enhancements
D NET,ID=*trle*	A TRLE for an unassociated ISM device will display **NA** for the PNETID.	Shared Memory Communications multiple IP subnet support (SMCv2)
D NET,TRL,TRLE=	A TRLE for an unassociated ISM device will display **NA** for the PNETID.	Shared Memory Communications multiple IP subnet support (SMCv2)

VTAM internal trace entries

For complete information about VIT entries, see z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT.

Table 165 on page 170 lists the new and changed VIT entries.

Table 165. New and changed Communications Server VTAM internal trace (VIT) entries for z/OS V2R4		
VIT entry	**Description**	**Reason for change**
ENFx	Updated to record the driving of an ENF exit for an ISM device.	Shared Memory Communications multiple IP subnet support (SMCv2)

VTAMMAP Formatted Dump changes

There are no VTAMMAP formatted dump changes for z/OS V2R4.

Tuning statistics reports

This topic lists the Communications Server SNA tuning statistics reports changes for z/OS V2R4.

There are no new and changed tuning statistics reports for z/OS V2R4.

Appendix A. Related protocol specifications

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

RFCs are available at http://www.rfc-editor.org/rfc.html.

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

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

RFC
Title and Author

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

RFC 653
Telnet output horizontal tabstops option D. Crocker

RFC 654
Telnet output horizontal tab disposition option D. Crocker

RFC 655
Telnet output formfeed disposition option D. Crocker

RFC 657
Telnet output vertical tab disposition option D. Crocker

RFC 658
Telnet output linefeed disposition D. Crocker

RFC 698
Telnet extended ASCII option T. Mock

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

RFC 727
Telnet logout option M.R. Crispin

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

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

RFC 734
SUPDUP Protocol M.R. Crispin

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

RFC 736
Telnet SUPDUP option M.R. Crispin

RFC 749
Telnet SUPDUP—Output option B. Greenberg

RFC 765
File Transfer Protocol specification J. Postel

RFC 768
User Datagram Protocol J. Postel

RFC 779
Telnet send-location option E. Killian

RFC 791
Internet Protocol J. Postel

RFC 792
Internet Control Message Protocol J. Postel

RFC 793
Transmission Control Protocol J. Postel

RFC 820
Assigned numbers J. Postel

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

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

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

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

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

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

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

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

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

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

RFC 862
Echo Protocol J. Postel

RFC 863
Discard Protocol J. Postel

RFC 864
Character Generator Protocol J. Postel

RFC 865
Quote of the Day Protocol J. Postel

RFC 868
Time Protocol J. Postel, K. Harrenstien

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

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

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

RFC 885
Telnet end of record option J. Postel

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

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

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

RFC 904
Exterior Gateway Protocol formal specification D. Mills

RFC 919
Broadcasting Internet Datagrams J. Mogul

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

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

RFC 933
Output marking Telnet option S. Silverman

RFC 946
Telnet terminal location number option R. Nedved

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

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

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

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

RFC 974
Mail routing and the domain system C. Partridge

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

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

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

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

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

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

RFC 1014
XDR: External Data Representation standard Sun Microsystems

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

RFC 1032
Domain administrators guide M. Stahl

RFC 1033
Domain administrators operations guide M. Lottor

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

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

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

RFC 1041
Telnet 3270 regime option Y. Rekhter

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

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

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

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

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

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

RFC 1058
Routing Information Protocol C. Hedrick

RFC 1060
Assigned numbers J. Reynolds, J. Postel

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

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

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

RFC 1073
Telnet window size option D. Waitzman

RFC 1079
Telnet terminal speed option C. Hedrick

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

RFC 1091
Telnet terminal-type option J. VanBokkelen

RFC 1094
NFS: Network File System Protocol specification Sun Microsystems

RFC 1096
Telnet X display location option G. Marcy

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

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

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

RFC 1118
Hitchhikers Guide to the Internet E. Krol

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

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

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

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

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

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

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

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

RFC 1179
Line printer daemon protocol L. McLaughlin

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

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

RFC 1184
Telnet Linemode Option D. Borman

RFC 1186
MD4 Message Digest Algorithm R.L. Rivest

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

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

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

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

RFC 1198
FYI on the X window system R. Scheifler

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 1270
SNMP Communications Services F. Kastenholz, ed.

RFC 1285
FDDI Management Information Base J. Case

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

RFC 1321
The MD5 Message-Digest Algorithm R. Rivest

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

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

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

RFC 1340
Assigned Numbers J. Reynolds, J. Postel

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

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

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

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

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

RFC 1354
IP Forwarding Table MIB F. Baker

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

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

RFC 1363
A Proposed Flow Specification C. Partridge

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

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

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

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

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

RFC 1387
RIP Version 2 Protocol Analysis G. Malkin

RFC 1388
RIP Version 2 Carrying Additional Information G. Malkin

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

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

RFC 1393
Traceroute Using an IP Option G. Malkin

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

RFC 1408
Telnet Environment Option D. Borman, Ed.

RFC 1413
Identification Protocol M. St. Johns

RFC 1416
Telnet Authentication Option D. Borman, ed.

RFC 1420
SNMP over IPX S. Bostock

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

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

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

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

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

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

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

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

RFC 1483
Multiprotocol Encapsulation over ATM Adaptation Layer 5 Juha Heinanen

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

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

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

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

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

RFC 1537
Common DNS Data File Configuration Errors P. Beertema

RFC 1540
Internet Official Protocol Standards J. Postel

RFC 1571
Telnet Environment Option Interoperability Issues D. Borman

RFC 1572
Telnet Environment Option S. Alexander

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

RFC 1577
Classical IP and ARP over ATM M. Laubach

RFC 1583
OSPF Version 2 J. Moy

RFC 1591
Domain Name System Structure and Delegation J. Postel

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

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

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

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

RFC 1647
TN3270 Enhancements B. Kelly

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

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

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

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

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

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

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

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

RFC 1713
Tools for DNS debugging A. Romao

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

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

RFC 1766
Tags for the Identification of Languages H. Alvestrand

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

RFC 1794
DNS Support for Load Balancing T. Brisco

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

RFC 1826
IP Authentication Header R. Atkinson

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

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

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

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

RFC 1832
XDR: External Data Representation Standard R. Srinivasan

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

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

RFC 1854
SMTP Service Extension for Command Pipelining N. Freed

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 1912
Common DNS Operational and Configuration Errors D. Barr

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

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

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

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

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

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

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

RFC 1995
Incremental Zone Transfer in DNS M. Ohta

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

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

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

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

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

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

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

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

RFC 2033
Local Mail Transfer Protocol J. Myers

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

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

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

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

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

RFC 2066
TELNET CHARSET Option R. Gellens

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

RFC 2096
IP Forwarding Table MIB F. Baker

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

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

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

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

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

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

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

RFC 2178
OSPF Version 2 J. Moy

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

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

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

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

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

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

RFC 2217
Telnet Com Port Control Option G. Clarke

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 2328
OSPF Version 2 J. Moy

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

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

RFC 2355
TN3270 Enhancements B. Kelly

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 2476
Message Submission R. Gellens, J. Klensin

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

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

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

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

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

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

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

RFC 2554
SMTP Service Extension for Authentication J. Myers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 2640
Internationalization of the File Transfer Protocol B. Curtin

RFC 2665
Definitions of Managed Objects for the Ethernet-like Interface Types J. Flick, J. Johnson

RFC 2671
Extension Mechanisms for DNS (EDNS0) P. Vixie

RFC 2672
Non-Terminal DNS Name Redirection M. Crawford

RFC 2675
IPv6 Jumbograms D. Borman, S. Deering, R. Hinden

RFC 2710
Multicast Listener Discovery (MLD) for IPv6 S. Deering, W. Fenner, B. Haberman

RFC 2711
IPv6 Router Alert Option C. Partridge, A. Jackson

RFC 2740
OSPF for IPv6 R. Coltun, D. Ferguson, J. Moy

RFC 2753
A Framework for Policy-based Admission Control R. Yavatkar, D. Pendarakis, R. Guerin

RFC 2782
A DNS RR for specifying the location of services (DNS SRV) A. Gubrandsen, P. Vixix, L. Esibov

RFC 2821
Simple Mail Transfer Protocol J. Klensin, Ed.

RFC 2822
Internet Message Format P. Resnick, Ed.

RFC 2840
TELNET KERMIT OPTION J. Altman, F. da Cruz

RFC 2845
Secret Key Transaction Authentication for DNS (TSIG) P. Vixie, O. Gudmundsson, D. Eastlake 3rd, B. Wellington

RFC 2851
Textual Conventions for Internet Network Addresses M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 2852
Deliver By SMTP Service Extension D. Newman

RFC 2874
DNS Extensions to Support IPv6 Address Aggregation and Renumbering M. Crawford, C. Huitema

RFC 2915
The Naming Authority Pointer (NAPTR) DNS Resource Record M. Mealling, R. Daniel

RFC 2920
SMTP Service Extension for Command Pipelining N. Freed

RFC 2930
Secret Key Establishment for DNS (TKEY RR) D. Eastlake, 3rd

RFC 2941
Telnet Authentication Option T. Ts'o, ed., J. Altman

RFC 2942
Telnet Authentication: Kerberos Version 5 T. Ts'o

RFC 2946
Telnet Data Encryption Option T. Ts'o

RFC 2952
Telnet Encryption: DES 64 bit Cipher Feedback T. Ts'o

RFC 2953
Telnet Encryption: DES 64 bit Output Feedback T. Ts'o

RFC 2992
Analysis of an Equal-Cost Multi-Path Algorithm C. Hopps

RFC 3019
IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol B. Haberman, R. Worzella

RFC 3060
Policy Core Information Model—Version 1 Specification B. Moore, E. Ellesson, J. Strassner, A. Westerinen

RFC 3152
Delegation of IP6.ARPA R. Bush

RFC 3164
The BSD Syslog Protocol C. Lonvick

RFC 3207
SMTP Service Extension for Secure SMTP over Transport Layer Security P. Hoffman

RFC 3226
DNSSEC and IPv6 A6 aware server/resolver message size requirements O. Gudmundsson

RFC 3291
Textual Conventions for Internet Network Addresses M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder

RFC 3363
Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain

RFC 3376
Internet Group Management Protocol, Version 3 B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan

RFC 3390
Increasing TCP's Initial Window M. Allman, S. Floyd, C. Partridge

RFC 3410
Introduction and Applicability Statements for Internet-Standard Management Framework J. Case, R. Mundy, D. Partain, B. Stewart

RFC 3411
An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks D. Harrington, R. Presuhn, B. Wijnen

RFC 3412
Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) J. Case, D. Harrington, R. Presuhn, B. Wijnen

RFC 3413
Simple Network Management Protocol (SNMP) Applications D. Levi, P. Meyer, B. Stewart

RFC 3414
User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) U. Blumenthal, B. Wijnen

RFC 3415
View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) B. Wijnen, R. Presuhn, K. McCloghrie

RFC 3416
Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3417
Transport Mappings for the Simple Network Management Protocol (SNMP) R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3418
Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser

RFC 3419
Textual Conventions for Transport Addresses M. Daniele, J. Schoenwaelder

RFC 3484
Default Address Selection for Internet Protocol version 6 (IPv6) R. Draves

RFC 3493
Basic Socket Interface Extensions for IPv6 R. Gilligan, S. Thomson, J. Bound, J. McCann, W. Stevens

RFC 3513
Internet Protocol Version 6 (IPv6) Addressing Architecture R. Hinden, S. Deering

RFC 3526
More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) T. Kivinen, M. Kojo

RFC 3542
Advanced Sockets Application Programming Interface (API) for IPv6 W. Richard Stevens, M. Thomas, E. Nordmark, T. Jinmei

RFC 3566
The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec S. Frankel, H. Herbert

RFC 3569
An Overview of Source-Specific Multicast (SSM) S. Bhattacharyya, Ed.

RFC 3584
Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework R. Frye, D. Levi, S. Routhier, B. Wijnen

RFC 3602
The AES-CBC Cipher Algorithm and Its Use with IPsec S. Frankel, R. Glenn, S. Kelly

RFC 3629
UTF-8, a transformation format of ISO 10646 R. Kermode, C. Vicisano

RFC 3658
Delegation Signer (DS) Resource Record (RR) O. Gudmundsson

RFC 3678
Socket Interface Extensions for Multicast Source Filters D. Thaler, B. Fenner, B. Quinn

RFC 3715
IPsec-Network Address Translation (NAT) Compatibility Requirements B. Aboba, W. Dixon

RFC 3810
Multicast Listener Discovery Version 2 (MLDv2) for IPv6 R. Vida, Ed., L. Costa, Ed.

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

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

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

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

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

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

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

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

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

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

RFC 4217
Securing FTP with TLS P. Ford-Hutchinson

RFC 4292
IP Forwarding Table MIB B. Haberman

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

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

RFC 4302
IP Authentication Header S. Kent

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

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

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

RFC 4308
Cryptographic Suites for IPsec P. Hoffman

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

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

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

RFC 4678
Server/Application State Protocol v1 A. Bivens

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 7627
Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension K. Bhargavan, A. Delignat-Lavaud, A. Pironti, Inria Paris-Rocquencourt, A. Langley, M. Ray

RFC 8446
The Transport Layer Security (TLS) Protocol Version 1.3 E. Rescorla

Internet drafts

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

Appendix B. Architectural specifications

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

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

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

The following RFC also contains SNA architectural specifications:

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

RFCs are available at http://www.rfc-editor.org/rfc.html.

Appendix C. Architectural specifications

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

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

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

The following RFC also contains SNA architectural specifications:

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

RFCs are available at http://www.rfc-editor.org/rfc.html.

Appendix D. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you can view the information through the z/OS Internet Library website http://www.ibm.com/systems/z/os/zos/library/bkserv/ or IBM Documentation https://www.ibm.com/docs/en. If you continue to experience problems, send a message to Contact z/OS web page(www.ibm.com/systems/z/os/zos/webqs.html) or write to:

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

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

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

Using assistive technologies

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

Keyboard navigation of the user interface

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

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, Japan

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

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

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the IBM Documentation. Use of hyperlinks in other output formats of this information is at your own risk.

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation Site Counsel 2455 South Road Poughkeepsie, NY 12601-5400 USA

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 document 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 measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com®/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

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

Minimum supported hardware

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

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Policy for unsupported hardware

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

Trademarks

Bibliography

This bibliography 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/systems/z/os/zos/library/bkserv/.

z/OS Communications Server library updates

Updates to documents are also available on RETAIN and in information APARs (info APARs). Go to https://www.ibm.com/mysupport to view information APARs.

- z/OS Communications Server V2R1 New Function APAR Summary
- z/OS Communications Server V2R2 New Function APAR Summary
- z/OS Communications Server V2R3 New Function APAR Summary
- z/OS Communications Server V2R4 New Function APAR Summary

z/OS Communications Server information

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

Planning

Title	Number	Description
z/OS Communications Server: New Function Summary	GC27-3664	This document is intended to help you plan for new IP or SNA functions, whether you are migrating from a previous version or installing z/OS for the first time. It summarizes what is new in the release and identifies the suggested and required modifications needed to use the enhanced functions.
z/OS Communications Server: IPv6 Network and Application Design Guide	SC27-3663	This document is a high-level introduction to IPv6. It describes concepts of z/OS Communications Server's support of IPv6, coexistence with IPv4, and migration issues.

Resource definition, configuration, and tuning

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

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

Operation

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

Customization

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

Writing application programs

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

Title	Number	Description
z/OS Communications Server: CSM Guide	SC27-3647	This document describes how applications use the communications storage manager.

Diagnosis

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

Messages and codes

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

Index

A

C

D

E

F

H

I

K

L

M

O

P

R

S

T

U

V

Z

Communicating your comments to IBM

Important: If your comment regards a technical question or problem, see instead "If you have a technical problem" on page 211.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM Documentation function
If your comment or question is about the IBMDocumentation functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Documentation Support at ibmdocs@us.ibm.com.

Feedback on the z/OS product documentation and content
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The title and order name of the document, and the version of z/OS Communications Server
- The section title of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Product Number: 5650-ZOS

GC27-3664-50